HITPC Privacy & Security Tiger Team with the HITSC Privacy & Security Workgroup Trusted Identity of Providers in Cyberspace Public Hearing Final Transcript July 11, 2012

Presentation

Operator

All lines are now bridged.

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good morning everyone, this is MacKenzie Robertson in the Office of the National Coordinator. Welcome to the Trusted Identity of Providers in Cyberspace Hearing, hosted by the HIT Policy Committee's Privacy and Security Tiger Team and the HIT Standards Committee Privacy and Security Workgroup. This is a public hearing and there will be time for public comment during the agenda and the hearing is also being transcribed, so I will just remind everyone who is speaking to please identify themselves. And instead of doing a formal roll, I think we'll just go around the table and everyone can introduce themselves and just state if they're on the working group or on staff. Thanks. Start with Kathryn.

Kathryn Marchesini – Office of the National Coordinator

Hi, I'm Kathryn Marchesini, I work with the ONC, so I help support the HIT Policy Committee Privacy and Security Tiger Team.

Kristen Ratcliff – Office of the National Coordinator

This is Kristen Ratcliff, ONC.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Joy Pritts, ONC.

John Houston – University of Pittsburgh Medical Center

John Houston, Tiger Team.

Lisa Gallagher – Healthcare Information & Management Systems Society

Lisa Gallagher, workgroup.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

Farzad Mostashari, ONC.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Dixie Baker, Privacy and Security Workgroup of the Standards Committee.

Deven McGraw – Center for Democracy & Technology – Director

Deven McGraw, Tiger Team

Walter Suarez, MD, MPH – Kaiser Permanente

Walter Suarez with Kaiser Permanente, member of the HIT Standards Committee and the workgroup on privacy and security.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Gayle Harrell, Privacy and Security Tiger Team and also the Policy Committee.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

David McCallie from Cerner, I'm on the Tiger Team and the HIT Standards Committee.

David Cassel - EPIC Systems Corporation

Dave Cassel from EPIC. I'm sitting in today for Judy Faulkner who is part of the Tiger Team.

MacKenzie Robertson – Office of the National Coordinator

And are there any workgroup members on the line?

Leslie Francis – National Committee on Vital and Health Statistics

Yes, Leslie Francis. I'm a member of the Tiger Team and the liaison there from the NCVHS.

John Blair – Taconic IPA

And John Blair, I'm a member of the Privacy and Security Workgroup.

John Moehrke – Health Information Technology Standards Panel (HITSP)

This is John Moehrke, a member of the Standard's Privacy and Security Workgroup.

MacKenzie Robertson – Office of the National Coordinator

Great, thank you everyone. I'll now turn it over to Dr. Mostashari for some opening remarks.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

Thank you all for being here today. I know several of you have been doing double duty, having been here for yesterday's Policy Committee meeting, and I thank you for the time and effort that many of you have taken to volunteer your time for another day and to be here. I also understand this is the first meeting of the joint meeting of the Privacy and Security Tiger Team for the Standards Committee and the Policy

Committee, so that's very exciting, like peanut butter and chocolate. We're here to discuss something very important today, trusted online identity for providers. And this is the way I look at this, we physicians have been given very special authorities and responsibilities in our society. We can announce someone dead, pronounce them dead and birth. We can access medical records, we can change medical records. We can prescribe medications that can be lethal or can be subject to abuse. We can bill commercially for millions of dollars and there is a level of trust associated with all those functions that have a very deep-seated regulatory protection throughout our culture for those. And yet, if we want to have physicians be able to do those functions, those same functions online, we need to be assured that the provider is who they say they are. That's what's at stake here, is to have a trusted system so that providers can feasibly engage in safe, secure, trusted online transactions for all of the above.

I know that there are important conversations in parallel to be had around trusted identity for patients, and we intend to work with the chairs of your workgroups to organize future discussions on that subject, but for before today's hearing, I would like to ask that we focus, that we focus on the provider use case. A use case that has tremendous opportunity, as I said, for ensuring trust, but also helping to create a marketplace, foster trust and help create a marketplace in its own right. Trusted identity for providers is not a new topic for the health IT Policy Committee, the Tiger Team or the Standards Committee Workgroup, but since the last time we looked at this issue, there have been some important developments. Two of the developments I want to mention are, and we're going to be hearing them at length, are the National Strategy for Trusted Identity in Cyberspace. Jeremy Grant is going to be speaking to us about that and this was really kicked off in April 2011 with the release of that national strategy for trusted identity in cyberspace and it really serves as a guidepost for public and private sectors to use when considering identity management strategies. It's based on four principles that you'll hear about that identity solutions should be privacy enhancing and voluntary, they should be secure and resilient, they should be interoperable, we love interoperable, and they should be cost effective and easy to use. And I think that is really very much in line with our market-based approach in general.

The other important update from a government perspective has been an update to the guidance issued by the National Institute of Standards and Technology that identifies kind of minimum technical requirements and what are the range of options for authenticating the identity of the users. I think this is called, NIST 800-63 R something. But, we had some important clarifications and updates made in December 2011 and we've gotten some now clarity in terms of how the market is actually implementing this guidance. We are going to have Tim Polk, Tim? Not here yet, who's the primary author of the guidance who is going to be here today and we have an entire panel dedicated to emerging private sector solutions, and really the other part of this is what's happening, what are the trends that are occurring? I guess there's two ways of looking at what we hope to accomplish here; one is to make it less likely a provider will have to have 20 different tokens to be able to access the hospital, relate to the health department, do e-Prescribing, talk to CMS, get into their EHR, get into the hospital's EHR, and so on and so forth. But the other way is that it's simply not going to be feasible to have that level of security, unless we make it a lot easier, unless we make it a lot less burdensome for providers and those who support them in terms of these solutions. Are we going to be able to make it feasible to have level three-identity assurance for providers? My hope and belief is that if it's not today, it will be very soon.

So, we're going to hear testimony and discussion about how quickly universal provision of interoperable level three identity assurance could be achieved, how feasible it is, what we're talking about in terms of burden, what vehicles, and I am expecting some robust discussion on all of these topics. But if there's one thing we want to stress is that the status quo isn't good enough, that we need to do more and we can't have continued delays in enabling providers to do online transactions to reap the benefits for convenience. But for access to these important tools, we can't have providers having their online identities stolen. We can't have the inefficiencies and frankly the lack of trust that can come with violations of those privileges. So, I believe it's possible for us to do that and I believe that today is going to be an important first step towards that. I'll turn it over to Deven and Dixie to take us through a recap of the work we've done in this space in the past years.

Deven McGraw – Center for Democracy & Technology – Director

Thank you very much, Farzad. It's great to be able to have a joint meeting on this topic with both the Privacy and Security working group of the Standards Committee and the Tiger Team of the Policy Committee because inevitably, we almost always in the privacy and security realm have…are faced with a set of issues that are both policy and technical components to it and we try to make sure we're in sync in our work largely through having some cross-membership. There are a number of folks around the table who sit on both working groups, which helps keeps us in sync. But in general, we also sort of, I think, fully understand that each of our domains of recommendation are a bit different. And so, I do, I think it's very nice to have us here together but what we will do from a procedural standpoint is, we'll have some time, I hope, at the end of this hearing to kind of collectively discuss what we have learned today, things that we think are relevant, and in need of further discussion. But we will not continue to deliberate as a joint group, but instead work within our respective committees, in order to T-up recommendations, as appropriate, if we have any, through our respective groups. So we're here together for the discussion and to borrow from one another's expertise, but we are not jointly together in terms of further deliberations after this day. But again, continuing to depend on the sort of, I always call it cross-pollination of the workgroup members that we have.

We're going to talk a little bit about, in just a second on these slides, some recommendations the Tiger Team has teed up to the Policy Committee and that the Policy Committee subsequently adopted on this issue, just so if there's kind of a level setting for all of the folks around the table, as well as members of the public who are listening about sort of where we've been before in this space, and you'll see on the slides that in fact we left a placeholder for reconsideration of these recommendations in light of

developments both with respect to NIST standards as well as the National Strategy for Trusted Identities in Cyberspace. And as Dr. Mostashari mentioned, that is in fact where we are. So, we'll go through that a bit and there are some bullet points as well for Dixie to chime in on what is relevant to these set of issues that the Standards Committee has done in the past. Dixie, did you want to say anything before I go through the slides? I know Dixie's going to take us through what the hearing is going to look like, so why don't you go ahead and do that.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

All right. Yes, I am very pleased that we're doing this hearing together. I think that this is really an important topic, particularly from the perspective that all security mechanisms that we have are directly dependent on accurate identity. Access control doesn't work unless you have the right identity. Audit doesn't work, digital signatures are ineffective unless you have the correct identity. And most importantly of all, a single sign-on can really be actually damaging if the original identity is not accurate. So this is a really, really important topic and I'm glad that we're having this hearing on this. We've put together four panels and the way we're going to run this hearing is that each of our panelists will have five minutes to make a statement, I won't call it brief, because five minutes is by estimation brief, will make a statement and after that, we will have open discussion. We do have a number of people on the phone, so we'll make every effort, MacKenzie, to make sure they have an opportunity to participate here as well. And with that, I think that we're ready to move ahead.

On the summary, it's an interesting point that Deven made, the interaction between the two committees. In the HITECH act, it actually says that the Policy Committee will make policy and identify priorities that the Standards Committee will then undertake. But in truth, the way ours works, it goes back and forth and in some cases we start with policy and they give it to us and we come up with standards. In other cases, we realize there is a need for standard and, oh by the way, we need policy really as a foundation for this and we sent it back over to the policy committee. So there really is an interaction. Okay, with that…

Deven McGraw – Center for Democracy & Technology – Director

All right, thank you Dixie. So, to remind us of where at least the Policy Committee has been before, just a few slides. So, several months ago we said...we made a recommendation that organizations that are seeking to exchange information as part of NwHIN, the Nationwide Health Information Network, should be required to adopt baseline user authentication policies that require more than just user name and password for remote access. So, not within your institutional walls or with your integrated delivery system, but when you're accessing remotely, although I think we also intended, when it's remote access into your facility, we wanted this to apply, too, So we said at least two factors should be required. And the definition that we were able to come up with for remote access is being defined as access over a public network like the Internet, but clearly probably more work needs to be done on that definition to be more clear about what we mean by remote access.

Here was some of our rationale for how we got to that point. We were not comfortable with sort of an application of the framework in the NIST standards or the specific DEA requirements, because of the stringency of the second factor requirement. We just really felt like that might be overly burdensome for

physicians to adopt notwithstanding that we wanted more than just a username and password. So we were a little bit stuck there. And we were particularly concerned again about remote access, but we had…again, we had a difficult time defining what remote meant. We also wanted to make clear that what we were recommending was really a baseline for authentication and certainly, there would be an ability for

organizations to adopt more stringent requirements although I don't think we fully thought through what that would mean when you're trying to encourage exchange within a network where one set of institutions has a higher set of requirements and others do not. And then we also acknowledged that for more sensitive, higher risk transactions that additional authentication of greater strength. Subsequent to that initial authentication, might need to be required as really has already been recognized with respect to the DEA policy regarding controlled substances. And we said we might have some additional work to do to sort of identify the use cases that might require that higher level of authentication.

Here's where we get to the point of this hearing. We said that these policies should be reassessed for consistency with other national identity efforts and technology developments, such as the National

Strategy for Trusted Identity in Cyberspace and also to address innovations in technology both within and outside the healthcare sector and I'll pause for a moment and let Dixie chime in on where the Privacy and Security working group of Standards has come down.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

This is an example of where the privacy and security workgroup recognized the need for a standard, but it really needed to be built on a foundation of policy. And we have, since we first encountered this topic, been consistent in our belief that policies and standards need to be at a sufficient level of assurance, as far as I've mentioned assurance level, to enable trusted exchanges between the private sector and the public sector. We still don't have a definitive answer on this, but we think it's really, really important, because

our largest healthcare payer and our largest healthcare provider are both federal agencies and its important these exchanges take place in a trusted framework.

Deven McGraw – Center for Democracy & Technology – Director

So then really the last two recommendations that we had was to direct ONC to develop and disseminate evidence about the effectiveness of various methods for authentication and reassess NwHIN policies accordingly. And then, of course, as far as the e-prescribing of controlled substances is concerned, certainly, physicians are going to need to have the capability to be able to do authentication consistent with the DEA rule, which the DEA is still working on, but we at least know where they are on an interim basis. Dixie.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

And people have mentioned to me that this two-factor authentication because of the DEA rule, really needs to be part of Stage 2 of meaningful use certification criteria, but we actually did…the Privacy and Security Workgroup actually considered that, but we decided with guidance from elsewhere, that we really didn't want…wanted to make sure we didn't go off on a different direction but would wait to see how the DEA rule ultimately comes down. At that point, I'm sure we will be adding a two-factor authentication capability to certify technology. And notice that that's a difference between the capability to do two-factor authentication and the policy directive that says you must do two-factor authentication.

Deven McGraw – Center for Democracy & Technology – Director

So that's it folks, for what we said previously. And we obviously…we really struggled with the

recommendations we came up with at the time, but we acknowledged that there were lots of additional decisions that would have to be made and that there were a number of developments in the pipeline that would probably be very influential on this set of recommendations, and we left room to reassess the policies accordingly. And so therefore, here we are today, to spend six hours learning from the field and hearing from folks who can help us figure out what we should be doing here, beyond what the law might already require. With that, were going to kick off the first panel, which I'm going to manage. The bios for each of the people who are presenting today are in the materials made available to everyone here at the meeting. I believe they are also online, so I'm not going to read them extensively, because they're quite impressive and we'd probably be here for the rest of the day. But I will introduce each person by name and title before they testify. We'll go in the order on the agenda. As Dixie mentioned, you only have five minutes, and it might seem like a long time, but it's ridiculously short. But certainly during the question period there'll be an opportunity for you to make points that you didn't get a chance to make in your statement. And we are, on the agenda, scheduled for a little bit of a break, but if we have some… we're not done with the questions, we may go over a bit, because the information is more important and if you need to take a break, you should do so. So with that, each of you will present first and then we'll go into questions versus having a question session after each presenter. So, first we're going to hear on the phone from David Hunt, who is with the physician steering group on trusted identity, as part of the Office of the National Coordinator on Health IT. David, can we hear you?

David Hunt – Office of the National Coordinator, Physician Steering Group on Trusted Identity

I think…let me ask you, can you hear me okay?

Deven McGraw – Center for Democracy & Technology – Director

We can hear you just fine.

David Hunt – Office of the National Coordinator, Physician Steering Group on Trusted Identity

Okay, that's perfect. Thank you very much. As you heard, I am David Hunt and I'm a practicing surgeon in the DC area and a medical officer in the Office of the National Coordinator and I was asked to help lead the workgroup that explored what could best be described as the use case of NSTIC for docs. As you've already heard the Department of Congress has been charged with implementing the National Strategy for Trusted Identity in Cyberspace, and put succinctly, as you've already heard again, this strategy really envisions a world that improves upon the passwords currently used to login online. It would include a private and a public market that issues trusted identity credentials. And, you can imagine in the consumer domain, the national strategy would allow an individual to be issued a digital credential that she might use to log onto her bank or e-mail, her social networking sites, all without having to remember different passwords for each because all participating in service providers will have agreed to consistent standards for identification of authentication, security and privacy. This system will be faster, more convenient, presumably safer and more private.

In the second slide you'll see the questions that we asked…we were asked to look at is, what's the day-to-day opportunities and benefits of having providers with such an identity credential? The workgroup consisted of myself, Debbie Bucci at NIH, at the NIH Center for Information Technology, Naomi Lefkowitz from NIST, Dr. Peter Bash at MedStar, Dr. Dirk Stanley at Cooley Dickinson Hospital, Dr. Darren Schulte at Apixio, Dr. Peter Rienzi who's at the Capital Care Medical Group and Dr. Jonathan Handler, CMI at M*Modal. In this third slide you can see we were able to identify a variety of valuable use cases and for this purpose, we have categorized them into three tiers or levels; if you could go back just one. The first or core level includes three uses of immediate apparent value, signing onto your EHR, signing into an electronic prescribing function and finally, having the credential to identify you as a provider for a health information exchange. Using such a credential or artifact to access your EHR can provide a common, convenient and secure access to one or, as in the case of us who practice at many locations, multiple EHR systems. At the level of health information exchange, such an identifying credential can be a uniform trusted and secure mechanism to provide access to an HIE and for electronic prescribing, this may, and I do have to emphasize may, as you've already heard, create a path that will improve the workflow for prescribing, particularly of controlled substances.

But beyond the core capacity such a credential could be used in the process of state licensing, board certifications or third-party payer participation programs and it could even provide an identifying key that an institution might leverage in various physician authorizations, such as access to a restricted patient care unit, like the ICU or in my case, the OR. The last point really highlights one important point that the workgroup discussed at some length, and wanted to make explicitly clear, namely that these uses are

constrained to the question of accurate identification and would, of necessity, have to be linked to other separate processes and protocols for authorization. That is to say this credential could be used to identify me as Dr. David Hunt, and any privileges and roles or authorizations that I might be granted, linked to and leveraged this trusted identity, but that is a wholly separate domain. And with this distinction, we can see a variety of third tier use cases, such as the identification for CME or education and training, professional society membership and even peer review publication authorship.

In this fourth slide, you can see just again what I've highlighted, some of the key benefits and core values.

And in this last slide, you can finally see some other possible uses of a trusted identity credential, such as this use to unambiguously identify an individual for performance measurement purposes and also compliance with regulatory matters. Now this was a very brief snapshot of the workgroups deliberations, and I will stop here to make sure there is enough time for other panelists and obviously I will be ready to answer any questions you might have. Thank you all very much.

Deven McGraw – Center for Democracy & Technology – Director

Thank you very much Dr. Hunt. You were quite efficient with your time, I appreciate it, but I'm sure there will definitely be some questions for you, I'm certain. Next we're going to hear from Alan Coltri, who's the chief systems architect for Johns Hopkins Medicine. Mr. Coltri, go right ahead.

Alan Coltri – Johns Hopkins University – Chief Systems Architect

Thank you and thank you for having me here this morning. Johns Hopkins is a fairly well-known name as that academic medical center. It's also the center of a six hospital enterprise and has large freestanding ambulatory services and clinics throughout the state. So we see the provider identity problem from a variety of perspectives. If I look at the history of this at Johns Hopkins Hospital itself, a number of years ago we constructed what we called a central physician directory. This we preloaded with a list of everyone, all the providers in the mid-Atlantic region; we began adding to that because our referral base, in fact, is worldwide. And at this point, years later, we are still adding about 250 providers a week. Every time we add a provider, someone looks that provider up in a variety of sources, calls their office, verifies their fax number, verifies their address, and verifies their national provider identity. So this is happening, we have an office where the people essentially do nothing else. We don't want to be sending data to the wrong person and we are forced to do all of this confirmation on our own.

It's also worth noting the clinical staff is heavily involved in research. At any given moment we have 4000 or 5000 studies underway and most of those studies, or many of them at any rate, have collaborators at other institutions. Every one of those studies includes some form of central site for data collection and essentially its own authentication mechanism, are you a member? Are you a member from the University of Colorado? We also have community hospitals, the problems in the community hospitals with identity are very, very different. Instead of large employed staff, you have a collection of 600-800 community physicians surrounding the hospital who have admitting privileges and these providers are, I think best thought of not as individual providers but as the heads of small enterprises with whom you have a business relationship. If you're looking at identity, it is not just the identity of the provider himself, but of his staff, of the person who's going to call in to your hospital system to make an appointment, of his

billing clerks. We are finding as we go forward that we need to know the identities not just of the principal, but also of the people acting on behalf of the principal.

Within our current systems we have the usual array of deployments. We have active directory, we have an LDAP directory. Over time many of our vendors have supported those, so our identity scheme has been gradually, over a period of decades, been coalescing around those two. We also have a web single sign-on product for all local websites. We have an enterprise single sign-on product, which we layer on top of our primary vendors. So we are involved in all of those activities as a means of providing some level of single identity. There is one area where we are doing something which is very similar to what you're talking about, but without the two factor piece and that's something called InCommon. Within the academic world, there is a Shibboleth-based federated security model that is widely used for sharing of resources in the academic world. We have hundreds of uses of InCommon going on at this point. One of the challenges that I think you're going to face on the remote access, is that there are, I have my cell phone right, what path is it using to get home? Is it using Wi-Fi? Is it using something else? Does it matter where I am when I use it? You know, the bring your own device thing, whatever you invent, people want to use these things and their pads and whatever you come up with has to be able to deploy to that new generation of device, as that device comes online. Thinking of things in the PC on the desktop, in the network, in the hospital, in the office is not going to serve you. I think I'm down to three seconds, so I'll stop.

Deven McGraw – Center for Democracy & Technology – Director

Okay, terrific. Thank you very much. Our next presenter is Rick Rubin, who is the CEO of

OneHealthPort, which is a health information technology management company based in Seattle. Go ahead Rick.

Rick Rubin – OneHealthPort – Chief Executive Officer

Thank you very much and good morning, I appreciate the opportunity to come talk to you today, and I've been asked to talk about the work we have done sharing provider identities across multiple relying parties. And in talking about identity, it's probably important to clarify that OneHealthPort has multiple identities. We are a commercial private company and that's the capacity in which we deploy the security service. But in the context of some fairly unique state legislation, we also are the lead organization for health information exchange and administrative simplification, and I'll touch on that briefly also. The security service was began at 2003 and it is designed to be a federated service for sharing provider IDs across

multiple relying parties. On behalf of those relying parties, we go out into the shared provider community and we register and bind to agreements the provider organization and a delegated administrator. And in mind of what Alan said, we very much have to focus on the entire provider team, not just for the

physician. We provision them with a digital ID, in some cases we provision them with second factors, and we can talk more about that in the question section if you're interested. We provide single sign-on across the participating relying party sites using that. We maintain those directories, and perhaps most importantly, we use that trusted community to drive increased adoption of those sites, that's really where the business value comes in.

In terms of results to date, the service, as I mentioned, has been working for about nine years. We have registered over 50,000 provider organizations of all types. So the very largest hospitals and practices

down to the solo practitioner hypnotherapist. We have well over 100,000 individuals registered within those organizations, we're taking people to about a million secure site visits a month. It's important to note that that service really focuses on protecting portal access, that's where we began and that's really the core of the service. We have approximately 25 different relying parties right now. They comprise a significant majority of the health plans in the Pacific Northwest, we also support some clinical sites, some quality measurement sites. The point was made by one of your prior speakers about how this can be useful across multiple settings. In terms of the benefits, I think you get two different faces. You have a provider face and relying party face.

On the provider side, they don't see this as having anything to do with security. This is a workflow tool. For the average provider organization to do their business with a diverse provider panel, they have to go lots of different places, and this is simply a way in their mind to simplify access to those sites, and they love it for that reason. They can open up and spend the day going back and forth without constantly being challenged. For the relying party side, there's probably two ways they would describe benefit, number one, they have outsourced their identity management headaches, so we take responsibility for that across a larger community and most healthcare enterprises don't necessarily have a core competency in identity management. But second, and probably more important for them, we use the critical mass, all those providers connected, we have excellent communication channels and what they really value is through the service, they see increased adoption of their online services. So again, that's probably the major reason we sign new people up is it gets their stuff used, because they had a connected community. I think the third benefit that should be mentioned is the community. Because we have this pretty pervasive credential out there and trust arrangement, we have a secure front door that we can repurpose so the secure credential provides the front door to the credentialing system we operate on behalf of the state, EHIE. It is used by quality measurement and performance measurement sites and so on. So it's been an asset that can be repurposed.

I'll talk briefly about some work we have done unto the HIE, I was asked to talk about some interstate and inter-HIE work we've done. HIE to HIE exchange, we are working with the HIEs in Alaska and Idaho and the Beacon Project in our own state, so we have four HIEs, and we have crafted and are in the midst of piloting an agreement that allows information to be shared. I guess you would call it a delegated model, where the HIEs agree to trust the HIEs based on the fact that the HIEs have bound their training partners, who in terms have bound their users. And again, that process is being piloted as we speak

between the Washington state HIE and the Beacon and between the Beacon in Idaho, it's very early. Just to finish up, I guess I'll leave you with a few key lessons learned. One, for us, single sign-on has been much more about the value of the business case and much less about the details of the security arrangements. And second, I think if you're working across enterprises or you're working in a community in a shared environment that is different in some subtle but very important ways, than being more enterprise focused. Thank you for the time and I'll look forward to answering any questions.

Deven McGraw – Center for Democracy & Technology – Director

All right, thank you very much Rick. And our fourth testifier in this panel is on the phone and I'm going to apologize in advance if I butcher your last name, Daniel Porreca is the Executive Director of HEALTHeLINK, which is a clinical information exchange, and HEALTHeNET, which is the administrative data exchange for Western New York State. Dan.

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

Thank you very much, you did a great job, by the way. HEALTHeLINK is the health information exchange for Western New York and we're also the lead organization for the Western New York Beacon. And as such, we recognized early on that in order to be of value for our community and to provide the value and to provide the capability of help in lowering costs and improving quality of care through health information exchange, we needed data, that was a critical asset. And very early on, some of our key hospital systems said to us, if we're going to make our data available through the exchange, we are not going to do it with a lower security level than what we require, and they required two-factor authentication, in order to get access outside their entity. So it was a pretty easy answer for us. We needed to implement a two-factor authentication solution in order to allow access to patient data via the technologies that we were standing up.

But what they also said, and these folks all make up part of our security committee, they said it doesn't make sense for the physicians in our community to walk around with the keychain full of fobs. We should have a method or a strategy whereby we have one solution for authenticating providers and then any entity that is part of that portal or that solution, will believe they are who they say they are, once they're at the front door, and that started us down a path for the development of our Healthy Community portal, which is a two factor authentication capability that we've stood up. In the interim we went live with two factor authentication utilizing one of the hospital systems existing capability. That was an interesting process and it had some mixed results, but it got folks kind of used to the fact that they're going to need to authenticate before they get access to the data.

In December 2010, we rolled out, December 23 to be exact, we beat the end of the year objective. We went live in 2010 with the healthy community portal, which was a lot more streamlined, it was a lot easier to access, and once we authenticated a user, provider or their staff for access to the data within HEALTHeLINK, they are authenticated for 12 hours. So there wasn't a need every time, if they walk away and come back 15 minutes later, they weren't asked to two-factor authenticate. And we've been able to implement technology that allows, you could either use a fob or a cell phone, a text message with the second factor authentication. And it's been very well received. The value proposition, from a community perspective, we now have the capability of standing up any number of entities within our framework. So, provider can come in, authenticate and then pick where they want to go, what entity they want to have access and there'll be a single sign-on kind of flow into that entity. They can then pop back out and go to another entity, so they can go to one of the hospital systems and then pop back out and go to HEALTHeLINK without having to authenticate again.

So the value for the provider is and will be just easier access for something they're not necessarily going to be happy about doing. We enhance the messaging capability, so we know the users are going to be coming to this one source for authentication that we can promote messaging. The ease-of-use, the lower cost, it is a lower cost solution for the community as a whole, because we can leverage the volume of more users and leverage that across. And for a patient, it's the comfort in knowing that we're doing

everything we can to assure the folks that have access to their data are who they say they are. They need to consent for providers to get access to their data. We're an opt-in community, we're an opt-in state, but we also are layering on this capability in order to ensure…give them the comfort level that we're doing everything we can to protect their data. And with that, I will it turn back.

Deven McGraw – Center for Democracy & Technology – Director

Okay, great. Thank you very much. All right, so now we're going to move into the question period. I will try to be mindful of making sure we're picking up responses from any of our panelists who are on the phone who want to respond to a question, but if I'm derelict in my duties, please speak up and then similarly, we will of course get to folks who were members of either of the workgroups who have questions on the phone. And, usually in the room it does help, I see David has his card up already, that does help me figure out who has questions, and since you were enterprising in getting that card right up there, you can go ahead and start.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Thanks Deven. This is David McCallie. My question is mostly for Dr. Hunt, but anyone else certainly should feel free to weigh in. The value of a shared and trusted identity is pretty clear, and has been well articulated by Farzad and by Dr. Hunt and others. I'm curious to know if there were any use cases where the value of anonymity for providers ever came up. And I'm not sure there are very many, but I wonder if that has been a practical concern in any of the actual implementations, where the provider wants perhaps to assert that they are a provider, but withhold their actual identity, for maybe reporting something they're concerned about, maybe some of the peer review models where you want to assert that

you are qualified to do the review, but don't need to provide who you are in doing the review. I didn't hear any discussion about the preservation of anonymity as an option.

David Hunt – Office of the National Coordinator, Physician Steering Group on Trusted Identity

Hi, this is David. Yes, we didn't discuss that at length. We did briefly highlight the possibility in cases where there were perhaps safety concerns that the provider might like to submit to either an anonymous

website such as the AHRQ mortality and morbidity website or some other patient safety functions; but, for the most part, that wasn't discussed.

M

And yet I'm not aware of any; it would seem most likely that the record of who was making the comment would be a system-recorded event even though it's not exposed. A comment that is untraceable is of dubious value in most cases.

M

Wholly not useful, exactly.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

This is David again, the NSTIC proposal actually makes a pretty strong case for the value of attributes that qualify an anonymous response or an anonymous behavior. So, you know that the entity making the assertion is qualified or appropriate to make the assertion, this is a core part of the NSTIC use case and it obviously has perhaps more applicability on the consumer side, which we're not talking about today. But my question was in the provider space, what's the value of that capability, to make assertions about your status if you will, or your qualifications to make a remark, but preserving or masking identity in the process. And I think you've answered my question. But, it is a core component that NSTIC and that's the basis for which I was asking.

M

No, I can appreciate that and as I said, I think the only instance might be in reporting some safety concerns, but even in that, I'm not really familiar with the many instances where anonymity would be so key. So, I don't see that as a huge domain within this.

Deven McGraw – Center for Democracy & Technology – Director

Okay, terrific. John, did you have your card up? Okay. They don't stick up very well, you have to sort of prop them.

John Houston – University of Pittsburgh Medical Center

I think Joy was saying…she taped mine shut so I couldn't ask any questions, which means Joy's a smart woman.

Deven McGraw – Center for Democracy & Technology – Director

Please make sure you pull your mics pretty close to you, maybe I'm just getting old, but I'm having a little trouble hearing folks.

M

Alan made an interesting comment about having to deal with issues of identity of the staff. And I guess I continue to wrestle with who is…what's the definition of the provider and how far down do we try to identify individuals and then having to wrestle with issues of autonomy of the individual providers and

having to manage staff and roles and the like. And I guess I would be interested in hearing comments about how we handle individual staff in this model, how we deal with roles and changing roles, especially if people change association with providers and how we make sure that's done in a way that is effective, efficient, isn't overly burdensome and again, provides the provider a level of autonomy that I think is important in terms of trying to manage staff.

Alan Coltri – Johns Hopkins University – Chief Systems Architect

I can't tell you the answer, but I can illuminate the problem a little bit. We are currently deploying an EPIC system at our hospital, in several of our areas, and we're dealing with the issue of how we incorporate the staff of the referring provider's office, the admitting provider's offices. Within the hospital systems that we're all familiar with, all these staffs have identities within the system and they all have roles and privileges to act within the system. So, that's all well-defined, and it may also be well- defined at their individual office; but when you start doing the boundary crossing, when you get to transactions like making an appointment or scheduling a patient to be admitted into a hospital, the physician doesn't perform that transaction himself. He orders it to be performed and it's performed on his behalf by staff. And that's really in the beyond authentication, it's in the roles. But the transmission of roles and authorization across boundaries is something that I think will be next on the agenda, once

we figure out who everyone is. Right now, I guess my cautionary note is, if you design a system, which is only about physicians, you have blown it, because we will immediately need to know about physical therapists and dentists and occupational therapists and nurse practitioners, and case managers, etc.. They will be immediately behind as soon as we try to do real work.

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

And just one comment, too. I think that to your point, an individual may be acting on a physician's

behalf in one instance and in the very next instance, they may be acting in their own right pulling data from a HIE, because they're a nurse or they're a physical therapist or a PA. So, it's clear that there could be changing roles almost instantaneous or least changing associations almost instantaneously and I think it's important to try to figure out how do we manage that.

Alan Coltri – Johns Hopkins University – Chief Systems Architect

I would tell you that what we have found is our focus has been at the organizational level for some of the reasons you know, we really bring individuals in through an organization. So we are vetting the identity of a provider organization and putting in place a delegated administrator and that individual is bringing on the rest of the team members. I would bet, I don't know if there's a statistic, but I would be if you looked at the total number of secure logins by health professionals in the country right now, only a small portion of those are physicians. There's far more work being done by staff and by other clinical team members. And the other part of that is as you mentioned, people have multiple affiliations at any given time. So part of the value, I think, that we have been able to add and we hear a lot from the relying parties is tracking the multiple affiliations. So when each organization is credentialed and then each individual user has a unique identity and they are tied to that organization, but they can also affiliate with other organizations.

So practices, for example, outsource a lot of their work and you have two people showing up at a secure front door saying I represent that organization, no I do. So, I would very much agree with your assertion that being able…whatever work you're going to do with identity management, it goes way beyond the physician and I think, again what we found is that it is more the tying of the individual to an organization than it is the tying of an individual to another practitioner, because by and large, the data you get to see has a lot to do with where you work. If I am a physician who works for this organization today I can see those patients. If I leave and go somewhere else tomorrow, I'm going to be able to see it different set of data.

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

Hi, this is Dan. I just wanted to echo and attest that the evidence that we have is very consistent with what has been stated. We do require staff of physicians to two-factor authenticate and the majority of the patient record lookups that are done are actually done by their staff on behalf of providers. So it's within…once they have been identified and authenticated, then it is within the role definition of the application that defines what it is they can do, what they can and cannot do.

Deven McGraw – Center for Democracy & Technology – Director

We have both Joy and Dr. Mostashari so their almost jumping out of their chairs here, so…

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

So, what we'd would like to focus on here is that first piece, there's been a lot of talk of authentication, but also what…the first piece here is the ID proofing itself and it would be really helpful for us to have…I think what I hear you saying is that you have to ID proof everybody who has access to the records or who is seeking that, is that one of the points we need to take away from this discussion?

Rick Rubin – OneHealthPort – Chief Executive Officer

Yes. I mean, every individual in the organization receives a unique individual ID and that requires them to have been…have their identity vetted and to sign an individual information sharing agreement that goes up to the organizational agreement, because the most minds that's where the responsibility lies.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Can I follow up a little bit on that? I think I heard you say that you do organization ID proofing and then you rely on the organization to do the ID proofing of its employees, is that right.

Rick Rubin – OneHealthPort – Chief Executive Officer

Well. So, when we bring an organization in for the first time we're verifying that organization and there's an individual who's got to be the first person in, this delegated administrator, and there is nobody in the organization to verify them, so we have to verify them. There are three ways to do that. By far the most common we use is knowledge-based authentication. They are receiving an online test, we've used two or three different models, and we've had some interesting experience with those different models. But the bulk of the people use knowledge-based authentication. Some people find that an invasive process, they don't want to do that for a work ID. They can always go to a notary public to be vetted. And then we've also found there are some people that don't want to do that either and we will, on a limited scale basis, do in-person identity verifications. Once the trusted administrator is in place, that organization has the ability to accept, if they want, delegated registration privileges and become an RA. We have found that 99.9% of the organizations do that because they feel they own that liability already, and then they can vet the additional individuals that they're bring in through their organization.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Do you have standards for what those organizations must do to vet their individual employees or do you leave that up to the organization itself?

Rick Rubin – OneHealthPort – Chief Executive Officer

We do, but we're going through thousands of organizations, most of whom who are small businesses and so we are essentially binding those organizations with an agreement that says they'll do the right thing. I certainly can't tell you that we go out and audit the processes they use. I think we found most of them are doing that anyway, they're talking about their employees, and I could go into more detail, I won't take the time unless you want, but in terms of how that individual user is actually credentialed, it requires the administrator to be involved in the individual through separate e-mails. We do some out of band verification of the administrator's identity and so one. And again, we can go into more or less detail if you want.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

If I may, this is Farzad Mostashari, if I may offer a suggestion. This is obviously, once you get a little bit into it, becomes deep quite quickly and the issues of identity proofing, next authentication and credential verification, and then role assignment and user-based access our separate but obviously, highly intertwined issues here. And what I would suggest is that for the purposes of today's discussion we are probably better served to focus on the first two rather than the third. So if we can get to a place where there can be a number of commercially available offerings for identity proofing and credential and authentication providers that different relying parties can use, that would be huge progress. I don't see us in the same kind of position to do that third part, where you determine what the roles are for the person, what their access rights are, what they're affiliations are, what they're organizations are, whether they…I think what we really need to focus on, even to talk about physicians versus nurses versus folks in terms of their roles might be, I think, a little bit of a topic that we could go really deep into and not find our way out of by the end of today, in terms of getting something concretely done. So what I would ask the group to consider, and maybe we can just do a check on this, is to say regardless of the role, what we're talking about is level three identity proofing and authentication. If you need level three for a nurse because they do those functions that have that level of risk, then it's part of the discussion, we don't care. If you're doing it for someone it for someone who's registering people and doesn't need level three, then maybe that's not part of the discussion. But I would want to ask the group whether that is overly narrowing in

the goals of getting progress made today, or whether that is inappropriate focusing? Mr. Coltri.

Alan Coltri – Johns Hopkins University – Chief Systems Architect

I wanted to ask a question that I think is related and we were talking about level three authentication as being required for remote access. The common phenomenon that we're talking about with many of these non-provider staff is a person who is in a secured environment, who was operating with systems in a secured environment and has not done two-factor authentication in that environment and is now reaching out to a foreign environment for data. Okay, so I guess I'm curious as to is that a remote access? If I am doing a system to system communication from a secured environment, does that count as a remote access?

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

I would again say we could have lots of policy discussions about what's appropriate policy guidance, best practice and so forth, and I am not sure that's the best…that's something we want to tackle.

Deven McGraw – Center for Democracy & Technology – Director

Not in the context of whether it's…this is Deven. Not in the context of whether it's an appropriate role for that person to play, but how do, assuming that in fact it will be staff who will be accessing data from the network outside of their own institution. How…you know, what is the…how do we insure that that person is who they say they are and maybe more to Mr. Rubin's point, how do we ensure that that person is from the organization that in fact has been credentialed to be able to access from the network? That to me is a completely legitimate question and gets to the heart of all of what we've been talking about. Not the question of whether that particular staff member is acting in her appropriate role, but rather whether when she does in fact go across the network, is she coming from the organization that we think she is and do we have the sort of chains of trust established, whether it's through…in the RFI for NwHIN they called it flow-down, right, where the organizations are responsible for credentialing the staff underneath of them in the way that Mr. Rubin described and whether you need to have standards for that or not is also a question on the table. But nevertheless, I think Mr. Coltri's question gets right to the heart of what we're trying to address today, which is that cross network query, what's the level, if any, and how do we assure that it's that organization or that person.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

…what I would suggest is for today that we not get into a detailed discussion of particular use cases, what's the level; do we need two for this or three for this or one, right? I'm saying, I think for today we should say take as granted that some people are going to need for some actions, they're going to need

that level of authentication. How do we create an ecosystem where there are many commercially available sources and many relying parties can rely on those credentials, without getting into today, a policy discussion, which is a fascinating policy discussion, about whether which particular use case requires which particular level.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

I would agree to that.

Deven McGraw – Center for Democracy & Technology – Director

Dixie?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Well actually, I was going to point out exactly what Farzad said, that there seems to be some confusion here among identity proofing, authentication of an individual to an identity that exists in the system and number three, assignment of the roles to that identity. And it is important that we focus on the first two at this hearing, you know, how you prove you are who you are to even get the credential to begin with and then, how, once you have presented that credential, how much proof you have to provide that you are who you claim to be and leave the role assignment to the side. It really is important or we'll never get through this hearing.

Deven McGraw – Center for Democracy & Technology – Director

I would agree. Is that a follow up on that comment David? Okay.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, this is David with just a clarifying question for Farzad and/or Dixie and then maybe for the panel. The bridge between authentication and authorization is sometimes the credentials that are carried across that are applied to you when you successfully authenticate. So I wonder if fair game for our discussion

today is what credentials are asserted about you as a byproduct of having been proofed and authenticated. For example, are you a provider…

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

…a credential can carry a lot of information, I certainly agree with that…but, and including role. But no, we're not talking about the role that's passed between an organization; we're talking about the identity that's passed between organizations.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So again, I want to come back to NSTIC, because you raised that as our framework. NSTIC makes quite a bit of noise about carrying credentials that assert things like, I am over 17 or I have a driver's license in the state of Kansas, as part of the value of NSTIC, which is the decoupling of assertions about what you are from who you are, if you choose to do that. And, I'm not so much focusing on the anonymity issue this time, now I'm just saying, what are the medical credentials…the credentials relevant to healthcare that might be built into the proofing and authentication process? Does it make sense, for example in your worlds that the single sign-on carries with it information that the current signing on user is a physician as opposed to is a nurse or is an office staff. Do you carry at that level of detail, does that matter?

Rick Rubin – OneHealthPort – Chief Executive Officer

This is Rick Rubin. We do, as part of…I think your distinction about identity proofing and authentication as opposed to authorization roles and so on, has been very similar to our experience. Our goal has been to have been to have a common approach to identity verification, identity matching piece and authentication. We then handoff a blob of information to the enterprise that contains a lot of detailed information, some of which you had described, but we absolutely believe that we have not met a single enterprise that wants to give up the authorization function, they own that. And similarly, we allow the provider organization to nominate and manage roles and affiliations. As a central party, we're never going to know that. So that is pretty simple, but that blob of information that gets passed is essential; if you're going to be the authenticator and somebody else is going to do the authorization, you have to pass the authorization system what they need to provide access, otherwise they're effectively going to end up redoing the whole registration, identity management and authentication to get what they need. So…

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So my…that's a terrific answer, exactly, much better and more clearly than I expressed it. What's in that blob, in your world, what do you pass?

Rick Rubin – OneHealthPort – Chief Executive Officer

So, in the short-term, we have a fairly hardwired blob, if that's not an odd phrase, and would that require a lot of consensus, and I can open my paper somewhere and give you all the details, but basically it is unique ID for the individual and the organization. It is tax ID, our experience has been that while everyone has an MPI, most of the relying parties don't yet have the systems to handle those, so they prefer tax IDs and a unique ID. It has a role and multiple affiliations, as I mentioned. It's not uncommon, for example, to find somebody in an academic medical center who has privileges a multiple places or the administrative personnel who have delegated responsibility to a billing organization. And we are now moving, we've had a number of requests, which we would hopefully will be able to honor later this year to customize that blob.

Going back to your point about authentication versus authorization, what they would like us to do is in some cases collect specific information on their behalf and pass it to them. They need the data, they don't want to have to manage the collection of data. This is particularly common with all the performance measurement stuff. So in terms of the organizations, they want someone to be credentialed to see X, Y and Z, but they don't just want anybody looking at their performance data; so they what specific pieces of information. So, that's how it the works.

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. Lisa and then Walter.

Lisa Gallagher – Healthcare Information & Management Systems Society

Hi. This is Lisa Gallagher from HIMSS. You know, at HIMSS we work a lot with the HIEs and I want to take this in a little bit of a different direction. Mr. Porreca, you mentioned…you made one comment that the system that you have in place gives the patients comfort. So what I was wondering is how do you communicate about a system like this to the patients? You know, part of the success of the HIEs is going to be the trust level that patients have with the whole system. And so how do you communicate to them and are you at this point able to have any measurement of the impact that communication might have on

patient trust.

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

That's a great question. I think the communication comes when the question is asked, how are you protecting my data. We're not going out with a campaign, you know with a billboard saying 2FA is here. But what we are doing is…and the question comes up, how are you protecting my data and we explain to them it's more than just a username and password and then kind of draw the parallel to the ATM card where you need something you have and something you know. So, I think that is the key to

ensuring that we're able to put their mind at ease on a case-by-case basis.

Deven McGraw – Center for Democracy & Technology – Director

Thank you. Walter?

Walter Suarez, MD, MPH – Kaiser Permanente

Thank you. I have two cards here. Thank you, so my…I think Dixie's distinction is a very good one in terms of focusing on identity proofing and authentication. So my questions are in those two areas because I think in most cases the identity proofing is a policy-based approach and the question really becomes, do we have standardized guidance for everybody to do the same type of identity proofing consistently? So, and there are two separate paths. One is the organization, as Alan mentioned, the internal organization, large organizations like Hopkins or Kaiser or others, and how they handle their identity proofing and authentication. And then there is the HIE world where things are going to happen externally to organizations. It sounds, Rick that you mentioned in your situation, you depend on the organizations to

do the identity proofing. Are there established, defined parameters, guidelines that everybody has to use in order to do identity proofing?

Rick Rubin – OneHealthPort – Chief Executive Officer

Yeah, again I would make clear, for the first person in, we do the identity proofing and then from that point onward, there are guidelines. But they're fairly general guidelines and we have found that has worked best for us. But there are fairly general guidelines and basically what we've done is said, this is…you need to do the right thing and you're going to sign an agreement that says you're going

to do that and accept responsibility for that. But you're right Walter, across the HIE world, that was part of what I meant in my comment of the difference between living in an enterprise with people you by and large control and can make do things and living in a community situation, where they don't necessarily have to or even want to work with you. If you make it too burdensome, they'll just do something else. So, you don't have the power to compel those folks and one other key point I'll raise, because I think it's important to recognize, that when you're talking about staff, in most practices there is a huge rate of

turnover. So if you start to think about how you vet, bind and provision, recognize these folks move around all the time. The turnover rate is extraordinary. So if you end up doing that every single time, that adds greatly to the cost.

So, we have a standard agreement that says you will use something similar to the following process to vet your people, and you will tell the truth and you will notify us when you find something that doesn't happen. And one of the biggest challenges there is because of turnover, it's really not even so much the vetting at the front end, it is the sun setting at the backend. You have people who are perfectly vetted and credentialed and that's great, and then three weeks later they are gone, and you have to have a process to sunset that person's access to the organization's data.

Deven McGraw – Center for Democracy & Technology – Director

We have some folks on the phone who haven't had a chance to chime in yet. So…John, you on the line?

John Moehrke – Health Information Technology Standards Panel (HITSP)

Yeah, this is John Moehrke and it's interesting, you kind of hit upon the topic I was looking at to…clearly we're talking a lot about provisioning users and making sure that there's a mechanism in place by which I can trust that this organization has provisioned their users. But, in the same way the provisioning of a user is important, de-provisioning them, when that user no longer is valid, no longer represents an individual at that organization, is just as important to the trust of identities and tied to that is of course,

dispute resolution where there were questions about identity and whether that identity was being used appropriately at a particular time. Are there some comments or discussion to further that use slide and the back end side?

Deven McGraw – Center for Democracy & Technology – Director

Go ahead, go ahead Mr. Rubin.

Rick Rubin – OneHealthPort – Chief Executive Officer

So that is something that we've struggled with. I've mentioned we have over 135 individuals across 50,000 organizations, many of them small organizations and a high rate of turnover. We've done a few different things; number one, lots of communication and outreach, reminding people of the responsibilities and the liability they have, if somebody they've provisioned, misuses that credential. Number two, I also mentioned that we use the trusted community as a communication channel. And so one of the things we do, as an example, we push out newsletters. When you push out electronic newsletters you to get bounce backs, and so one of the things we do is, we go back and say oh, we got a bounce back, is that because you have a spam filter or is that maybe because that person has left the organization. There been a variety of techniques we've developed like that to try and nudge people in that direction. We also try to monitor usage. So if you notice a whole bunch of people…if you notice one organization doing thousands of inquiries, there's probably one person, there's probably credentials being shared. So there are a variety of things you can do to monitor, to nudge. Ultimately when you're

dealing, and again that community view, not an enterprise where there are employees who are accountable to you, but when you're working from the community view, it's monitoring, it's education, it's communication and using other methods to try to encourage people to solve that problem.

Deven McGraw – Center for Democracy & Technology – Director

I'm going to go, Gayle hasn't had a chance, but we'll get to you, we're kind of blowing through our break again, so if people need to take one, take one. Go ahead, Gayle.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Thank you Deven. That brings up the whole issue on enforcement and how do you deal with the bad player? Once you have identified someone who is a bad player, how do you deal with that and what are the consequences of that behavior?

Rick Rubin – OneHealthPort – Chief Executive Officer

So in our case, fortunately, at least we are not aware of extremely bad behavior, so we have not had to deal with those types of consequences. We've certainly had circumstances where we have suspended credentials. And the real punishment, if you will, is that people use our credential, not that there's anything wonderful about the credential, but the content it protects is very important to their business. So being denied…having their organization denied access to that information, really causes them pain and that is probably the most profound consequence if your credentials are suspended, that you lose access. We have not been in the circumstance of having to pursue actions with law enforcement or to engage in any form of civil litigation to date. So it's more, we reach out, we notify, we suspend the credential, we ask to see some indication that the behavior that was observed has been fixed and that is not a totally satisfactory approach, but that's how we've pursued it to date.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead Gayle.

Leslie Francis – National Committee on Vital and Health Statistics

This is…can I ask a question on the phone?

Deven McGraw – Center for Democracy & Technology – Director

Gail has a follow-up and then I'll call on you.

Leslie Francis – National Committee on Vital and Health Statistics

Great, thanks.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

One quick follow up. You've not had any legal action against different people or criminal action against people. Have you had any major data breaches?

Rick Rubin – OneHealthPort – Chief Executive Officer

Key point here, we do not sit on…we do not own any data and that we are simply taking people to the front door and saying…vouching for the fact they are who they say they are, authenticating them and passing that information along. We have not been involved in any breaches because of that identity management service. And again, very important to note that we do not own, hold or sit any data, so we would not have that breach issue.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead, Leslie.

Leslie Francis – National Committee on Vital and Health Statistics

My questions were along the same line and in many respects have been answered, but, from the perspective of NCVHS, one of the questions that came up in the hearing we had was what patients know about who has access, particularly in the context of, if there's someone who's trying to trace someone, an abuser, people could be seriously injured if the wrong person follows up and finds out say where they're living.

Rick Rubin – OneHealthPort – Chief Executive Officer

It's interesting. I mentioned that we vet the organization and one of the reasons we do that is probably the most common challenge we find is organizations that do not have rights to view health plan eligibility data are interested in doing that to get access to the demographic information. We have, in terms of that case that was just presented, we have dealt with organizations from the state that collect child support and who do have appropriate access to that information based on the court orders and so you do get into those different kinds of use cases. But, I would agree that it's very important to consider not just sort of the violation of an individual's medical privacy, but the other negative ways that demographic information and healthcare records could be misused such as a domestic abuse situation.

John Blair – Taconic IPA

Yeah, this is John Blair, I had a question.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead John.

John Blair – Taconic IPA

So, I just wanted to go a little bit further on the de-provisioning providers that have access when they leave an organization. Outside of monitoring, do you have any other active processes for timely de-provisioning those providers?

Rick Rubin – OneHealthPort – Chief Executive Officer

Our process is, again, that responsibility is delegated. We frankly have no way of knowing, that's the key. Again, lots of turnover. We have no way of knowing that Rick Rubin is no longer employed by a small clinic in Eastern Washington, and so, it really comes down to binding the organization, binding the individuals, holding them accountable and monitoring. There's no other real follow-up unless we are made aware of something. Sometimes we have the circumstance where we see somebody who had a credential in another place, now has moved over and now wants to get a credential there, too. So, that's another way of monitoring.

John Blair – Taconic IPA

So when you say binding, are you talking about contractually binding them?

Rick Rubin – OneHealthPort – Chief Executive Officer

Yes, both at the organizational level and at individual level. We use a common contractual framework that every organization, every individual and every relying party executes.

John Blair – Taconic IPA

Okay.

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

This is Dan. We follow a similar process, we have a participation agreement with all the organizations in our community that have access to either as a data source or as a data recipient. And it really is up to the covered entity to make sure those users that are de-provisioned are…we turn off their ID, but we also have a process by which we show the authoritative contact or authorized contact, who it is that has access within their organization and it's up to them to make sure that those folks are all legitimate users.

John Blair – Taconic IPA

And what's the timeline for notification?

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

Well, I'm sorry.

John Blair – Taconic IPA

What's the timeline for notification?

Daniel Porreca – HEALTHeLINK and HEALTHeNET – Executive Director

From a contractual standpoint, it should be immediate, upon…for the person leaving their organization. They should be notifying us and turning off the access, although that's not necessarily…there's really no way for us to know that.

John Blair – Taconic IPA

I would assume they're in breach if they don't. Okay, thank you.

Deven McGraw – Center for Democracy & Technology – Director

Thanks. We're going to try to take a couple more questions in the room, but we are reaching the end of the time for this panel, so, John Houston?

John Houston – University of Pittsburgh Medical Center

A follow-up on an earlier comment. I think in terms of identity proofing, one of the concerns I guess that I have or, I think, one of the key requirements is how do we ensure the level of identity proofing satisfies regulatory bodies, such as the DEA, if this is ultimately going to be used for prescribing of controlled substances and the like. How do we ensure that they're satisfied with what is being established is sufficient to identify the physician to the prescription by example? How do we make sure that there is

satisfactory authentication to comply with regulations?

Rick Rubin – OneHealthPort – Chief Executive Officer

I think from our perspective, we pick the universe where we felt we could add value, we can move sort of a large group of people at least a little way up the assurance chain, and we recognize that by doing that, we were not necessarily going to be able to meet the very highest levels. With the increase in e-prescribing and the second factor requirements around narcotics, we've been spending a lot more time talking to second factor vendors who have creative ways of solving that problem. But in the short-term candidly, we don't feel that…we have not been able to come up with something that satisfies the very highest levels of everybody's expectations and can be broadly adopted in the real world community. And so we've made some compromises there, with the goal that if we get them all roped in, and vetted, then it's a little easier to start moving them up the chain, as they see value in doing that, that's the key.

Deven McGraw – Center for Democracy & Technology – Director

Joy?

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

There's been a lot of discussion about within the community or even within a very large enterprise, like Johns Hopkins, that individuals move around a lot. Every time that individual moves, do they have to be…do you have to ID proof them again? For example, Mr. Rubin, you were talking about a large community and said that people come and go all the time, but often times they are just taking another job within the same community. So, right now, do those people need to be re-ID proofed every time they take a new position?

Rick Rubin – Chief Executive Officer, OnHealthPort

So in the perfect world, we would not have to do that. Today, yes, if I am working for Dr. Jones, I'm a staff person and Dr. Jones' administrator has vetted me and provisioned me, and now I quit Dr. Jones and go across to Dr. Smith, they're going to have to go through the process again because it's important to tie me to Dr. Smith's organization. Now, they're going to do that through their delegated process. I'm not going to have to go through an external process for that purpose, unless again I was going to Dr. Smith and I was the first person in because that was a new practice. At some point in the future, it would be nice to be able to take advantage of some of those…arrangements, but to the degree you're asking the

organization to accept accountability, in some cases they're vetting the person anyway as they employ them. That's the answer they give us.

Deven McGraw – Center for Democracy & Technology – Director

We're…David, is it a quick one because we are just about out of time.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, it's just an elaboration on John Houston's question, mainly for Mr. Rubin. Can you envision the model that works well in your community scaling so that other communities, which adopt a similar model, would be trusted by your community for those relatively uncommon, but non-zero cases when things cross communities? How do you scale this…

Rick Rubin – OneHealthPort – Chief Executive Officer

Well, we've raised to that a little bit with our H2H agreement, and here's what I would say. There is no amount of software or paper that will compel people who don't want to solve problems to solve problems. And I will say, and there are a lot of people who don't want to solve problems or who want to raise the ultimate edge case to explain why you can't ever do that. I have 100% confidence that if you have communities who want to figure out a way to do something, and I think this H2H project, you can absolutely do that. Our service has now expanded to Oregon and Idaho. So, when people want to find a

way to buy in, I think there are lots of good ways to do that and to expand circles of Federation. If you've got somebody who wants to raise all the reasons why things can't happen, you're not going to solve that problem.

Deven McGraw – Center for Democracy & Technology – Director

So true in so many contexts. That was a perfect way to end. I want to thank the panelists for taking the time to share their knowledge and their expertise with us today, much appreciated. It's quite possible we'll come back to you with some additional questions, if that's okay, but you're certainly excused from being on the hook today and we'll do a quick transition to the second panel, which Dixie will run, and we'll just keep right on going. Thank you.

M

Thank you.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

For those of you on the phone, we are just waiting for our panelists to sit at the table and then we'll begin. Right. Thank you all for appearing on the panel two for us today, we appreciate it. Panel 2 is entitled Trusted Identity, a Changing Ecosystem and we have three speakers on this panel. The first speaker is Jeremy Grant, who's a senior executive advisor for identity management at NIST, the National Institute For Standards and Technology and he manages the establishment of what we've referred to several times already in this panel, the National Program Office for the Implementation of the National Strategy

for Trusted Identities in Cyberspace or NSTIC, and we're really pleased to have you here today. The second speaker is Jim Polk, hi Jim. Jim is a computer scientist at…Tim Polk, hi Tim, a computer scientist at NIST and his focus is on cryptographic security mechanisms, and he is one of the authors of the NIST special publication 800-63 that Farzad mentioned earlier, that was just released of January 2011, so we're pleased to have you here today as well Tim, thank you. And the third speaker is Deborah Gallagher who is with the General Services Administration, and she is the director of the Identity Assurance and Trusted Access Division there at GSA. We're very pleased to have you here. So with that, Jeremy?

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Thank you. Well good morning and thanks to the members of the committee for taking the time to hear from as today. We're really looking forward to the opportunity to share a little bit about what we have been doing in different parts of government to try and drive the notion of trusted identities in the marketplace forwards, both in the federal government as well as in the commercial sector, and certainly in ways that impact health IT. I wanted to start the conversation off by really throwing out a vision for say four years from now, and let me amend the slide, it was written as 80% of doctors and patients, I think it's clear from the last panel we need to look beyond doctors to health providers. But if four years from now the majority of health providers and patients were carrying some sort of a secure credential, say that it was bound to their smart phone for identification and authentication, and organizations not just in health, but really across the marketplace could trust that credential, in lieu of the existing username and password systems that are so prevalent today.

The solution would be interoperable with legacy login systems, meaning that organizations wouldn't have to worry about provisioning new credentials, dealing with things like password resets. They all support strong, multifactor authentication, getting away from the weakness of single factor passwords. The credentials would be tied to some sort of a robust identity proofing mechanism, meaning that you actually know people are who they claim that they are, given that last week was the 19th anniversary of infamous dog on the internet in the New Yorker, that could be a nice advancement to have. And finally, the technologies would be built from the ground up with privacy in mind so you'd have both a set of rules and policies that govern the use of information in them, as well as technologies that were actually part of this enhancing, to ensure that privacy wasn't really a question in terms of how these technologies could work.

What would this actually mean for improved security and for breaking down barriers to online service delivery? Well, a few numbers that I thought were helpful to throw out from security, Secret Service does the study jointly with Verizon every year, looking at data breaches and the causes of them. Last year five of the top six vectors of attack were actually tied to passwords and there's a variety of different ways that passwords can be exploited for data breaches and other bad teams in the security world. But when you look the five of the top six, and you look at stats that came from the Secret Service showing that 82% of records that were compromised last year, were compromised through attacks tied to passwords. It tells you that we really need to get away from this technology that has really outlived its use, and that the fraudsters and criminals who are trying to do things in cyberspace take advantage of our weaknesses are turning to this more than any other vector. No surprisingly, with this, Javelin put out the study showing that there was a 67% increase in the number of Americans impacted by data breaches in 2011. And unfortunately for the Health sector, Symantec put out a study showing that health sector was the number one target, accounting for 43% of all data breaches in the US.

Clearly we have some problems that need to be addressed. What we want to do though, is not to tackle it in a way that's going to address the security aspects, but also can we design an ecosystem, a marketplace of solutions that can break down barriers to delivering different types of services online. Obviously it's very difficult to provide a lot of, and share different health PII if you don't know who's a dog on the

Internet, and we've talked about that already in this last panel. We also need to ensure that these systems are baking in privacy by design and that it's highly usable, rather than being something doctors and others in the community are going to run away from because they simply don't want to deal with the hassles. It's also worth sharing the number, in terms of what average consumers deal with on the online environment. There's a great study on the shop.org site talking about how 54% of consumers will leave a site and not bother to return if they are asked to create a new account, and I'd ask folks on the panel and others in the room to think of how many times you've shopped online until you were asked to provide a little slug of information and said, why bother. And interestingly, 45% of consumers will abandon a site if they forget their password, rather than actually attempt to reset it or answer any security questions. The systems that are out there today are not considered very user-friendly and it's just not worth the bother.

So, the National Strategy for Trusted Identities in Cyberspace outlines the path forward. Some background on it, it had its roots in President Obama's 2009 cyberspace policy review, where when they were looking at major cyber security issues in the country, not just in government, but also in the broader marketplace, they seized on the issue of identity and cyber security, specifically looking at some of the

problems with passwords, like the ones I outlined earlier from the Secret Service study. And so one of the short-term action items that was called for in the President's review, was the creation of a cyber-security focused identity management vision and strategy, looking not just at the security issues, but also one that was designed in a way to address privacy and Civil Liberty's interest and try to leverage new privacy-enhancing technologies for the benefit of the country. The strategy itself was signed by President Obama in April of 2011, at an event that was hosted at the US Chamber of Commerce and both major industry players as well as privacy advocates were on stage to actually endorse its release.

At the end of the day, the NSTIC is really trying to catalyze the marketplace, an identity ecosystem as it's dubbed in the strategy, where individuals and organizations can better trust each other everyplace they go online because they're following agreed upon standards and policies to authenticate digital identities. And as far as I'd mentioned earlier, there are four guiding principles that really drive all the work that we're doing as we catalyze this marketplace, which is that the solutions that emerge must be privacy-enhancing and voluntary, they must be secure and resilient, they must be interoperable, and they must be cost effective and easy to use. So, the vision for 2016, and I think we'll actually see elements of the ecosystem much sooner, so that you have an ecosystem where individuals can choose from among multiple identity providers and digital credentials for convenient, secure and privacy-enhancing transactions anywhere at any time.

I want to take a bit just to talk about the privacy aspects because privacy enhancing is one of the four guiding principles. A key aspect of NSTIC, and this is actually getting a little bit to some of the things that I think David was talking about earlier, is how can we create identity management solutions that can minimize sharing of unnecessary information, shifting the focus from say a credential that shares tons of information, to really only those specific attributes that a reliant party would need to know. I do want to say that while there's a lot of great work being done in there, we don't have a marketplace that supports that readily today. Crafting that and catalyzing it is one of the things we're actually trying to focus on within the implementation. The NSTIC also prescribes adherence to Fair Information Practice Principles, of FIPPs, which I think are pretty well known to folks in this room, to ensure that the solutions in fact have privacy built-in and that this identity ecosystem isn't used as a way to somehow be removing choices from individuals and sucking more data out of them, as we've seen in some applications today.

It's also voluntary and private sector led, there's nothing mandatory about it, individuals can choose not to participate and those who do participate can choose from a variety of what are envisioned to be both public and private sector providers. It's also important to note, this is really focusing on catalyzing a marketplace, and there isn't any single government central database that's being created to keep track of transactions. We get asked that a lot from folks who are suspicious, because the government's doing

something in identity; this really couldn't be any further from, I think, where most people have concerns where this could go. And also, one goal is to preserve anonymity and pseudonymity online. There are times its okay to be a dog on the Internet, particularly in types of applications where there really isn't any risk if you are anonymous or operating under a pseudonym. I think everybody agrees that the ability to do so is actually one of the things that has fueled the growth of the Internet and its ability to be a great medium for free speech and freedom of association, and there's nothing around NSTIC that's actually trying to change that.

In terms of what NSTIC calls for, it's really a private sector led effort at the end of the day. It's in no way a government run identity program, the White House published a strategy, our role in this is really to work on facilitating collaboration among different private sector stakeholders as well as stakeholders in the government, to create this marketplace. There was recognition when the strategy was crafted that the private sector is going to be in a much better position than the government to drive the specific

technologies and solutions that comprise the ecosystem, and that frankly, if the government tries to specify certain technologies, we'd probably fail. There are simply too many entrepreneurs in the space, you'll have a chance to hear from some of them later on the panel today, who are pushing the boundaries. We really want to focus on what the strategy should look like in the end state, to focus on specific outcomes, not specific technologies. What we are looking to do from the government side is provide support. I am hoping later today, we'll be able to announce the award of a two-year grant for an organization to serve as the secretariat for a new privately led identity ecosystem steering group, which will be set up as a private organization, either a dot.com or a dot.org, with government participation, but ultimately they are to convene all stakeholders from across the country including, we hope, many of you in the health sector to work on crafting consensus standards and policies along with an accreditation process for identity providers, that will comprise the identity ecosystem. Also, the government, since we tend to spend money on a lot of these systems ourselves, we do want to act as an early adopter, to stimulate demand.

So, it's important to know, when we sort of talk about NSTIC and the end-state that we're driving to in a few years, relative to what exists today. NSTIC lays out a path for the future, it's a strategy and aspirational document that points out what online identity should look like in the next couple of years. Today, and you'll hear much more about this from my colleagues Tim and Deb, but under the FICAM program, which is leveraging the work NIST has done around special pub 800-63, looking at guidelines for electronic authentication, there are a number of private sector trust framework providers that

offer solutions today. I won't spend too much time talking about it, since Deb will really be getting into it in detail, other than to point out that government for a couple of years now, has already been working on, in fact, there's been a ton of work on a system to actually accredit different private sector credential providers for use in the dot.gov realm and there's actually a pretty vibrant and growing marketplace based off that. It's the trust framework provider adoption process is something that's maintained by Deb Gallagher and the folks who run the FICAM office at the GSA. And it's really doing some fantastic things, it's provided a certification process where there wasn't one just a few years ago.

And that is something I wanted to talk just a little bit about in terms of good news. There is an emerging marketplace today. Three years ago if you were looking at third-party credentialing solutions, you were looking at just a few technologies and form factors, and no accreditation process. So if you were buying something…well, you were buying something, but you had providers that might self-assert that they actually met certain requirements, it didn't mean that they did. Today, on the technology side, we're seeing things like mobile devices catalyzing a wide range of new solutions that are smashing through some of the previous cost and usability challenges, and making strong authentication easier to deploy and use. Tim will talk about the latest version of 800-63, recognizes a lot of advancements in the marketplace. It's really a much more flexible document than the first iteration, which a lot of our partners in the marketplace have been excited about. And the certification process that's in place now allows folks to buy both in government as well as outside, to buy solutions knowing that they've actually been certified against the NIST requirements.

Some key drivers to talk about in terms of what we've seen in the marketplace, particularly that impact the health community. For starters, there's an interim final rule that was published in March of 2010 by the DEA, for electronic prescribing of controlled substances, which specifically called out a new version of 800-63-1, and the identity proofing mechanisms that were used there, as the standard that needed to be followed if you were a physician prescribing controlled substances. Last year when 800-63-1 was published, NIST made sure to recognize the trust framework provider adoption process the GSA runs, as the one and only certification process that we recognize at NIST in terms of being able to actually assert, to certify that commercial solutions are meeting the requirements NIST has set out. And Tim will also talk about the standard itself, or the guidelines itself, and some of the changes they made.

Late last winter and early spring, GSA certified Kantara and SAFE BioPharma as the first two trust framework providers for non-PKI level of assurance 3 solutions. I do want to note while we're talking about non-PKI and LOA3, we shouldn't overlook level of assurance 4, which is the highest level that is prescribed by the NIST guidelines, that's basically when we're talking about hardened tokens like the Smartcards that I carry and use for access to government systems. It's worth noting that NIST released a new draft of that standard yesterday, FIPS 201, which would allow for these credentials, which are very heavy and very hard…actually light, but very hardened and quite heavy when it comes to security, to be used to create drive credentials on mobile devices. I think it's going to provide a whole new range of additional models that can be used for strong authentication in the mobile world. We saw Verizon become the very first non- PKI level 3 certified identity provider in November; there are several others that are in the queue and, quite importantly, Center for Medicare and Medicaid services outlined plans in February to also support all FICAM approved credential providers, which now means, from an impact perspective, in the short-term, a physician will be able to use the same GSA certified credential both for electronic prescribing of controlled substances as well as to access applications at CMS.

So long-term I think the question that I would pose to the Tiger Team and others who are looking at how to solve the broad identity conundrum in health IT, is why not look to leverage that same standards credential elsewhere in the health ecosystem. Supporting this sort of standards-based approach really drives a virtuous circle, because you have standards and an accreditation process that's out there, you have more certified credential providers. The more certified providers that are out there makes it much easier for more relying parties to accept those certified credentials, and that in turn drives a better business case for even more providers to enter the market, bringing more variety to the types of technologies that are offered and driving down the cost. The alternative, obviously, that every stakeholder can go continue to go it alone, which means health providers may have to carry three or five different multifaceted credentials to use in different applications; usability and security will suffer and as adoption lags, the business case erodes for anybody to really be in this market. So, we think the answer is pretty clear and we're certainly working from our side to drive things forward. I mention that the steering group that we're standing up, the first meeting of it is tentatively scheduled somewhere in Chicago, our Secretary, once the grant's awarded, will actually announce when, during the week of August 13. We encourage health community stakeholders to show up as you guys have an important voice at the table and we really want to make sure your perspectives are heard. We do expect as well, to be announcing probably in early September, the award of about ten million dollars' worth of NSTIC pilots, at least one of which, I don't want to say too much, but may actually focus on the healthcare sector, and depending on how things go forward, I'm pretty excited about the direction those are moving on, and the government continuing to work as an early adopter to stimulate demand. So, with that, I'll skip the last slide, since I know we're tight on time and I'll hand things over to my colleague Tim.

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

Thank you very much for having me here to talk about NIST 800-63-1. I think most people here probably have heard this document discussed, perhaps not positively, hopefully at least some of…takes time. I want to give you a quick overview of what the current version has in it, what the changes are and why we actually needed to do this document in the first place and why we've had to do an update. The real goal for doing this document actually was very, very narrowly focused. We were responding to a memorandum from OMB, policy memorandum 0404, which said there's…which provided requirements to agencies to classify electronic transactions into four levels and then to implement authentication that met those levels or that was consistent with that for all of their applications. They were very concerned, there were a few applications that were fielded where it turned out that, in retrospect the authentication requirements had not been really thought through very well. One of the consequences of this memorandum was that since we didn't want agencies to have to reinvent the wheel and figure out what those requirements really were at each level over and over again, NIST was tasked with developing complimentary technical guidance.

This is actually not a document that NIST wanted to write. In fact, we really, really didn't want to write

this document, because there's a lot of art to this document as well as the science. I'm from the cryptographic technology group, we're very comfortable in being able to say that this algorithm is the work factor to break this algorithm is two to the 80 or two to the 128, we like those kinds of numbers and it's very difficult to do this with a lot of the authentication mechanisms that are out there. And our requirement was that we write a document that looked across the broad range of authentication mechanisms and ranked them into these four levels, which are useful, but not as precise again as we might have like. But, we are troopers and we did as we were told and we wrote this document, which was NIST special publication 800-63, which provided a framework for remote authentication over an open network. I'd like to say that my personal metric, and we are metrics organization at NIST, my personal metric for success is when organizations that are not required to use NIST documents voluntarily choose to do so. I have to say we were very pleased and very surprised at the response to NIST special pub 800-63 because as we said, we did not feel that we had not done as scientific a job as we like to do. It was more art than we would have preferred when we finished the document, but we found we filled a void and people have

been using this. And so we've been very excited about the response.

That said, the original document and even the current document certainly has some warts and that's why we've done a revision and we'll go through that a little more extensively. So, the response to 800-63 was really in two parts. One of them was people loved the document and they wanted to use it and there were a bunch of things that they really disliked about the document and they sure hoped we would fix them right away. And the major problem with the original version of 800-63 is that it was very prescriptive, we were trying to give agencies a cookbook that they could go through, check the boxes and know that they had done what they needed to do to satisfy their requirements. We expected at the time that agencies were going to be issuing credentials themselves. The world has changed over the past seven years and things quite didn't work out the way we expected. But there were a lot of pieces and there were also a lot of technologies that have evolved since that time, ones that we kind of thought were sort of researchey, a little bit leading edge, and we weren't trying to push agencies to the leading edge at the time 800-63 was published. But, technology moves quickly and a lot of those technologies are now no longer theory…no longer research.

You may be familiar with the 800-63 authentication model. When you get down to the simplest model, there's really only two parties. If you issue the credentials and you also own the application, you're the relying party, you're basically every one of those except for the subscriber or the claimant in the middle. But we did, at the time we were working on this document, envision a more complicated, a richer

ecosystem where you could use credentials…where at least it was plausible that you were going to use credentials issued by another party. And to be honest, I think this is actually the much more prevalent model then that very simple model that we were expecting at the time that we put this together. A lot of people talked about level three authentication, level four authentication today. Really levels one and two, where we either have no confidence that you are who you say you are, or very little confidence, they are easy, they are not interesting. The place where the rubber meets the road is trying to achieve level three and level four authentication and these have proved somewhat difficult in practice, although we're doing far, far better and we have a lot more possibilities today.

But level three and level four are both multifactor authentication. So, I'm just going to, in the interest of time, flip on to what's new in this document and also what's been missing. I think this is the meat of what I really wanted to say here. 800-63 as I said, was very prescriptive, it had a limited number of technologies that it recognized and it tried to be sure that it provided the simplest possible framework for going forward. And part of the reason was, there was no expectation that there would be third parties that could help with that process. The authentication technologies were limited. We have a lot of new types that are in there in 800-63-1. We also have a much more generalized support for using tokens in combination. There were a couple of what you could think of as combined combinations that were recognized in the original version of 800-63. 800-63-1 is much more of having the matrix and being able to choose one from column A and one from column B, and put the two together. There are some limitations on that, we're going in the classic, something you know, something you have, something you are and trying to make sure that those combinations are not two of one of those categories, because then we don't think we've really added anything.

But we're trying to be much more general. We've also added a lot of detail on assertions; assertions were sort of emerging as the way to do things, but SAML assertions and related technologies…we've seen them become increasingly important and we've tried to provide a lot more detail about how to do assertions and how to do them at higher levels. Derived credentials, which Jeremy already mentioned, is also new in 800-63-1. Personally, I have three level three credentials that I use at NIST. I have my PIV card, I have a hard RSA secure ID token and I also have a software secure ID token on my blackberry. Any of those use can be used to achieve level three. I don't expect some of that to go away, that I'm going to have to have more than one credential. What derived credentials is trying to attack is the problem that all three of those level three credentials I have require that I do in-person identity proofing. There is no reason for that. We should be able to leverage one high-quality token to issue other tokens without repeating the in-person identity proofing, and do that much more cheaply. For example, once I have my PIV card, I really should have been able to establish my software one-time password token on my blackberry without making an appearance. Derived credentials, as envisioned in 800-63-1 fixes that problem. It also provides a mechanism to help aggregate some of the problems with tracking down those credentials at the end of lifecycle. So that if my PIV card is revoked, there's a way to link it to the other credentials that exist for me. Right now I have three completely independently issued tokens, which is going to require three independent processes to control them at the end of the lifecycle. So, that can be improved. As we noted, there is the FICAM managed assessment process. This is really important because this really makes it possible for agencies to use third-party issued credentials, because they don't have to go out, do an assessment, and try to understand. Now that 63-1 is more general, it's a little more complicated to make that assessment so it's very important to have that third party.

One of the things I didn't note in…we didn't change the picture in the model, that model that already had five different components. But we did talk in the document about the possibility that identity and attribute providers could be separate and could be combined in this process. We see that as something that's going to go forward, being very important. We did not expand most of the treatment of the document to talk about that, because frankly, we desperately needed to have a final publication. We put the document out as draft two or three times, it was trying to go final. And I just…so that was the small way to fix that problem. I know I am over on my time, but I would like to note that there are two things that are still missing in 800-63-1, and I think that you might want to know why. Knowledge based

authentication where at lower levels instead of issuing a credential and doing any kind of identity proofing, you simply allow a user to answer a few questions about themselves is something that we do

not support in 800-63. The reason for that is that any information that you as a credential provider can pull out of a public database, someone else can pull out of a public database as well. We just have not found a way to be sure that we really had any level of confidence that credentials or access that's provided that way is trustworthy.

Remote biometrics is something that we actually have more hope for, and we think it's a very exciting idea; however, remote biometrics have a lot of problems still today in terms of aliveness detection and securing the remote channel and we…it's a technology that we don't think is quite ready. We are hoping that we will work and we've been exploring ways that we can work with the biometrics community to see some of that technology move forward, and we hope that someday, that will be in future versions of 800-63. So, I know we can't take questions now. I thank you for your time. I did want to include in the slides a few URLs and some points of contact. Elaine Newton and Ray Perlner are my primary co-authors on the most recent draft, and they're actually your best sources of information. They respond to email much more quickly than I do these days. So, thank you again. I'll pass it to Deb.

Deborah Gallagher – Office of Government Wide Policy, U.S. General Services Administration

Okay, thank you.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Thank you Deborah.

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

Is this close enough? Can you hear me? I don't have any slides today. I just wanted to you talk a little bit. I think that Jeremy and Tim have both set the stage pretty well as far as what the ecosystem envisions as well as what 800-63 is. And, I have to say that FICAM relies on 800-63 a lot. So, I think all of you know we have three different programs that came together, it was e-Authentication, PKI and HSPD-12. The PKI and HSPD-12 both look at the identity proofing of individuals and how you go about doing it. As part of the HSPD-12, there was a special…excuse me, a FIPs publication develop 201, which Jeremy mentioned the new release just came out yesterday. But all of that goes into, this is how you identity proof someone, these are the controls that you need to have in place, this is the card and the credential. So, that's in place. PKI is a part of that which again, gives us a higher level of assurance that somebody is who they say they are, and that was combined with the effort for e-Authentication to be able to authenticate electronically across the network. And that was all brought together in a group and the result of that was the federal identity credential and access management roadmap and implementation guide, the FICAM.

So, the first use cases and the intent of the roadmap was published in December, 2009. We've had a…we put the implementation guidance in there which will now have to be modified because of the new publications. But we put implementation guidance in there last year, in 2011. So, these were some of the things that we brought together and the intent was to have consistent identity proofing, consistent issuance of credentials and a way that was trustworthy across the executive branch of the federal government. Well, what happened was, after that we discovered that there were a lot of people that liked the consistency and they liked having the guidelines, but they were not a part of the executive branch of the government. So, a couple of other things came out and the first thing, not first in chronological order, but one of the things that came out was the specification for PIV interoperable credentials. And those credentials are very, very similar to the PIV credentials, but they're for people or entities that are outside of the federal executive branch. The US Senate is going to be issuing PIV interoperable credentials. Banks, there are several issuers that are doing that, state and local governments and the their people, their personnel who that interact with the federal government or even with each other and need a high level of assurance of the identity of an individual, will be able to use these credentials. So that's been going on, we have several PIV-I providers.

The second thing Jeremy alluded to, and that's the trust framework provider adoption process. This started out in the non-PKI world. So PIV and PIV-I are both PKI, this started out as being non-PKI and levels of assurance of identity proofing that matched the 800-63. We took schemes that were available in the industry, so the standards that were out there SAML, username and password, IMI, whatever. We took those and adopted them, but with a little bit of modification to include things like the privacy and security concerns that the federal government has. So out of that scheme adoption came a profile. And then the profile was included, so we had a profile and those were the technical layer of it. After that, we said, okay, we're not…we as the federal government are going to be able to look at and evaluate and assess every identity provider that's out there. So, how do we go about attacking this, because we are

going to expect a lot of identity providers to be coming out of the woodwork. So what we did was we adopted the trust framework from industry. We took different ones and we assessed them and looked at them, looked at the procedures that they have in place, looked at their processes and said, you guys, the way you're doing things, we trust you and you have been assessed to go out and in turn assess the identity providers, to make sure that they are following the guidelines, to make sure that they are using the profiles that have been identified so that we are enhancing the security, or at least protecting the security and protecting the privacy of the individuals that are being identity proofed. So you can't share the person's

individual information from one entity to another, unless you have specific agreement from the individual holding the credential, the identity credential.

So, we did all of this and the first…came together and we assessed three different providers or trust framework providers; one was Kantara, OIX and then the last one was InCommon. That was great, it worked well, except we kind of, and this was a mistake on our part, we didn't expressly say which of the

privacy controls we needed to have in place. So, we had trust framework providers that were there and they were ready to get to work and approve identity providers, but then we went, oops, we have to add these other areas. So there was a perception that the privacy controls that were from the FIPs, I never can remember the FIPs, it's the privacy principles, that we…their thinking was that maybe this was just too cumbersome, they couldn't do it. But, the trust framework providers looked at all of the people that were being reviewed as identity providers and they realized that it really wasn't as big of a problem as what they thought. And these identity providers, as long as they are going with the intent of 800-63, that they

were doing the things we wanted them to; again, they needed to be abiding by the profile that had been established and the profile included the 800-63 requirements for identity proofing.

So, we got over that, so we have three trust framework providers. There are multiple identity providers out there that have been approved at level 1. When we really started looking at accepting these externally issued credentials, based on the memorandums from the CIO last October, we realized we needed to get things going here. And we started realizing when the agencies went back to their organizations and looked at what they needed as a relying party and the level of assurance in the relying party, it became apparent that level 1 was probably not going to be as effective as we what we had hoped it would, and we wouldn't get the traction. So, there has been a change, somewhat, in the trust framework provider process and they came to…one of the providers came to NIST and GSA and asked if they could take the components of identity proofing and all the different levels of assurance. So, if you're looking for level 3, say there are ten different components, ten different things that have to occur before you can say they are level 3. And they can take…different industry partners can…or different groups can say, okay I am going to do these six, and another group can say, I'm going to do these four and they partner together to achieve all ten of them. So, we're calling it a componentized approach and that's being worked right now, so that different entities can use their level of expertise and their core competencies and join with other groups that have different core competencies to have an end-to-end service that gives us a good understanding and trust level of the level of assurance, the identity proofing.

So, we have that, that's relatively new. Jeremy mentioned it briefly, we are looking at other agencies to have a service of some kind, we haven't quite defined it yet, so that the acceptance of all these externally issued credentials can be more easily done. So that there may be a service so that, I don't know, VA will accept credentials from an external entity and it will be accepted also by IRS. You know, things of that nature…with a little bit of additional identity proofing, if it's required, probably won't be, but you never can tell, and that way the end user, the citizen, can more easily access government information. So, I think I'm running out of time, but there are a lot of efforts going on, some of it federated, some of it is just changing with the times so that these different credentials can be accepted. I will tell you that there are several entities out there, like I said, that are PIV-I providers that are also looking at being level 3 providers that may or may not include PKI and you can go either way with level 3. Thank you.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay, we ready for questions. I think I'll use the chair's prerogative and ask Debra one…since she just now covered this. You mentioned certification by components.

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

Components of the requirements.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right.

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

So, yes.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So if you do a certification with multiple components, is the certification over the integrated set of components?

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

Yes.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay, just want to thank you.

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

I'm sorry, I mis-mentioned that.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay, thank you. Wes?

Wes Rishel – Gartner, Incorporated

I apologize for getting in late. I think I heard among the three speakers the representation that there are now firms out there doing these trust evaluations at various levels and that there's enough work going on that it's a business, it's sort of out of the experimental range. What does it cost someone, if my mother wanted to go in and get herself trust identified, what would she pay?

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

So, the way that this works, as I understand it is that the company that wants to get certified has a range of laboratories, shall we say, of organizations that they can negotiate with. But that they negotiate a price based on the complexity of the solution that they're trying to have evaluated and it's a competitive market, although it's not as competitive as we would like because there's not as many players. Because of the way it works, the government is not involved and I don't know, it's not cheap, I'm sure. I mean you're looking at…I'm sure that as the level of assurance goes up…what I am saying is that it's a

business investment that you're making. Whatever it costs, I'm sure that the businesses think it's too much. It's something that they end up having to make the decision that they can amortize it over the business that they're going to be able to generate. But, we don't have the hard numbers for you.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

The one thing I can say…so Google actually was one of the first at a level of assurance 1, just username and password. You can now sign on to government sites, rather than create your own user name and password for low level of assurance, you could use your Google ID. They actually blogged about it on their site and I think they said they spent about $5000 or $6000 on the assessment. To go through LOA-3, where you're actually dealing with real identity proofing, real multifactor authentication, there are now two organizations, Kantara and SAFE BioPharma that are both qualified as assessors at LOA 3. Verizon's actually talking later and they can probably tell you much they spent on it, I think it was significantly higher because it was a much higher level of assurance that they had that could certify that.

Wes Rishel – Gartner, Incorporated

So, 600,000 physicians, give or take a couple of hundred thousand…

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Wes would you…(indiscernible)…thank you

Wes Rishel – Gartner, Incorporated

…millions of other clinical providers who have every reason to access IT systems, you know, are we talking…let's just say a round number of three million, okay. Are we talking about $15 million dollars, 300 million dollars? Three billion dollars

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Are you talking about how much the credentials will cost...the certification process for the providers?

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

…just need one each or 20 each?

(laughter)

Wes Rishel – Gartner, Incorporated

I'm just trying to get…

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Sure, so, let me say what we're seeing from business models in the commercial marketplace, because NSTIC's very much focused on…while we are part of the government and working with our friends in the government, what we're really trying to do is stimulate activity in the commercial sector. And one thing we have not actually seen yet is the emergence of any one definitive business model that is going to

be the dominant one. And, it's actually something we've avoided getting too much into. There are some firms who will sell you, as a physician a credential for X dollars, and I think you'll have a chance to hear from some of the providers later today, so you could probably ask those questions. There are others who are willing to basically give you the credential for free, and their business model is that they want the relying parties, every time you're authenticated to pay a transaction fee. And, the latter is quite interesting in terms of where we're seeing a lot of different private sector stakeholders starting to collaborate around the idea of what would that model actually look like and how could you come up with a true business model for both identity exchange as well as attribute exchange and what would different relying parties be willing to pay for it.

Google's often talked, just as one example, about identity for the cost of a postage stamp, because they found that in the health community, I think they actually used an example, Eric Sachs, who's one of the identity guru's over there, they went over to Stanford around the corner from them and looked at Stanford's hospital, that in order to be…what they will do today to validate that a patient is actually somebody, is when you sign up online, they'll have your address on file and they will send you an envelope for the cost of a postage stamp, that will give you a one-time verification code that you'll then enter to get into the Stanford site the first time, and they consider that…whether it would meet the guidance of this committee or not…they consider that to be a reasonable way to de-risk the possibility that somebody's trying to spoof that person's identity. So based around the notion of identity for the cost of a stamp, you are seeing a lot of different firms start to come together to develop business models on a transaction basis.

Wes Rishel – Gartner, Incorporated

Yeah, that's for patients.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

For physicians as well. Again, I think some of the providers who are speaking later today, the credentialing solutions may tell you what their thoughts are on business models. And I'm pretty sure there are folks who are in the room today who'd want to charge an upfront fee and those who would look at something a bit more of a managed service and then amortize the cost over several years.

Wes Rishel – Gartner, Incorporated

I'm just going to guess it won't be the cost of a postage stamp.

(Laughter)

W

Probably not.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Kind of following up on what you asked Wes, I know that there's one business model where blocks of identifiers are sold to a company and then the company takes on the responsibility to identity proof and provision them. Is that specified…for example, what the identity proofing, what it requires in order to

get a block, what a company signs up to do in order to provision these, is that specified in the regulation?

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

So, special pub 800-63 does provide the framework, it provides a set of minimum requirements at each of the levels for identity proofing. What it does say is that through level 3, identity proofing can be performed remotely. At level 4 you have to come in in person. So that that's the most distinct breakout . I would note that identity proofing by the cost of a postage stamp is, in fact, one of the things that is incorporated in various ways into the remote identity proofing. One of the ways at level 2, you can confirm that the applicant is who they say they are even after issuing the credential, at level 2 you can do it by sending them a letter at their official mailing address that says "hey, we issued you a credential. If something's wrong, please contact us immediately." And at level 3, you would send them a mailing that would be required to use to complete the process. This isn't as popular because when people do remote identity proofing, they want to make it be completed right at that time. But in this scenario, you would send a letter to the person's mailing address that said, "here's the code that you need to enter to complete your process."

So, we do use that as one of the possibilities. It's one of a number of possibilities though, so, we try to give a set of possibilities with some flexibility, but if you know what level you are trying to issue credentials at, if you're going use 800-63 as your framework, we are fairly clear that here's the minimum requirements for how you would go forward. It is one of the sections of the document that actually was expanded considerably because we do know more about identity proofing than we did seven years ago and what we really know is that it's hard and we need to be as flexible as possible. So, it is something that we've tried to address in the most current version.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Let me just stress one other point here. Wes was commenting, it may be more than the cost of a postage stamp. That may be, but if you can leverage a single credential that's standards-based across multiple relying parties, then you can actually amortize the cost of that credential to the point where on a per transaction basis, it may actually be below the cost of a postage stamp. A lot of what we are trying to do with NSTIC and FICAM is create standards-based frameworks where a solution can get certified, say by GSA, as meeting the NIST technical requirements and then can be used across a variety of applications. So if I am a healthcare provider, I don't need to get one credential for e-Prescribing of controlled substances, a second one to access CMS and a third one to access the private health IT system that I'm going to get. We think we can really generate network effects and generate some real economy to scale, if you can have a standards based approach that actually drives interoperability credentials across systems.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

We're going to hear from the private sector service providers, Wes and we can drill down into different business models, as well. But, I just want to note from the three federal agencies and officials there, it's really a tremendous amount of optimism, I think, from where we were three years ago, two years ago where we held our last hearing through a combination of actions that each one of you and Jeremy I think summarized this really amazingly well in his key drivers slide, slide 10, where he noted, I think maybe even before this right, the very publication of the 800-63-1. The dash one on the flexibility that Tim mentioned, the DA e-Prescribe rule, NIST recognizing the FICAM trust framework and FICAM actually providing those assurances, GSA then certifying Kantara and SAFE BioPharma as trust framework providers for non-PKI, LOA3, Verizon providing non-PKI LOA 3, and with many others in the queue and then CMS, as we'll hear. So these are all, I think, real enablers and facilitators of what we in the federal government can do to unlock this both for the federal government's own use, but potentially creating and helping to create an ecosystem.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Just to follow up on what Farzad said, industry will tell you the number one thing that they actually want is for both the government and other key industry groups to actually pledge to support these types of standards based approaches. People have been talking about this kind of stuff for years. I am not that old, but I've been in this space since 1997 and some of what we are talking about today were the kinds of things we were talking about back then and for a lot of different reasons, mostly because the idea was either ahead of its time or there were technical or policy barriers in place, these things failed. What we're seeing now as more and more stakeholder groups are buying into the NIST spec, buying into the FICAM accreditation process, looking at the strategies the President signed around trusted identities in

cyberspace, we have vendors calling our office each week who want to come in, not to try and sell us something, because we're not actually buying anything in the NSTIC Program Office, but to let us know they're watching all of this and they're coming in to essentially reveal a little bit about their product roadmaps and how they're actually working to align the next generation of products around the strategy and around the FICAM and the NIST framework. That's a remarkable thing, it's really having an impact on the marketplace and as Farzad said, you would not have seen it three years ago.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

David?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

My questions will leverage that a little bit, those thoughts. I want to reflect back to the closing comment of the previous panel, where the comment was made that no amount of technology will solve trust issues when somebody wants to get in the way and not let it happen. And so, my question is really about the scaling of trust to NSTIC envisioned levels of universal trust, I think was the phrase that you used in your presentation, Jeremy. I'm speaking mostly to you, but certainly anyone else can feel free to weigh in. And my question is, what do you think are the remaining barriers that inhibit us from actually getting to what you described as being available in concept anyway in 1997. And is it Wes's issue of cost? Is it complexity of level 3 proofing and the fact that that's still ambiguous and painful to some people? Is it lack of a standard? Are we missing a key component in the standard? Is it lack of an agreement about what credentials should be passed back and forth, even though we have standard ways to pass those credentials back-and-forth? What's the barrier that keeps this from happening all the way?

M

The answer is yes.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

There's a number of barriers. If I would had to break them down, I would say there's probably five. One has been some of the business models and cost issues that have been out there. In the past, unless you were in a particular regulated industry where you needed to get one of these credentials in order to access certain systems, many organizations would find that the cost of just doing this for single use credential wasn't worth it. And tied closely to that has been the lack of standards for interoperability that we're finally starting to get beyond as the industry is maturing and the governments been trying to help them mature. Usability has been the third big challenge. In the past, when you had a solution that required somebody to carry around a standalone token, a lot of times users, certainly in the consumer space, weren't exactly fond of that and in many cases rejected it. The amount of innovation going on around mobile devices, now that the bulk of the population's carrying smart phones and taking advantage of capabilities in there, is really starting to get around that. As Tim mentioned, at NIST we have a soft token that's just a map on our Blackberry that we use for RSA secure ID and it sure beats the old key fob that I used to have, which I used to leave in my desktop half the time and then I couldn't get in at night to do work, made my wife happy, but, caused some problems in terms of productivity.

The other two issues, I would say, are privacy. When you start talking about these identity solutions, a lot of questions get raised about how much information is being shared, how much is harvested, collected and stored. There had not been firm policies in place that actually dictated what the privacy posture of

these solutions would be. And, a very big one that I certainly wouldn't want to gloss over, is liability. Who gets sued if something gets cracked or if something goes wrong? If you look at say the bank card world, you have reg E and reg Z for credit cards and debit cards that prescribes what happens if , say your Visa card is stolen. It basically states that you as the consumer are liable only for $50 and the rest is basically split between the issuing bank and the merchant who was at the point of the fraud. Now some people talk about the need for a liability immunity. I don't think that necessarily is a workable a model as liability certainty, which is what you see in the bank card world where now you as a consumer and the merchant and the bank all sort of know what the risk is and what you might be liable for and you can start to model those risk into the transactions. Coming up with something similar in the identity world, I think, is going to be quite important to allowing some of types of transactions that we want to see, particularly in the consumer space go forward. All five of these are things, by the way, that we intend to tackle in the identity ecosystem steering group that convenes next month, and we'll be working over the next few years to craft a framework of standards and policies for the ecosystem.

Let me address one other thing, which is the concept of sort of universal trust. I don't think we're going to get it overnight and while NSTIC envisions that we'll eventually be there, to borrow another bank card analogy, I think what we'll really see are the creation of different trust frameworks in different sectors that will then unify over time. So specifically, what I'm talking about with bank cards is, think about ATM cards 20 or 25 years ago. First you had a card that only worked at your bank. Then you start to look at this logo on the back that said Cirrus or Star or Plus or Most and you'd see an ATM on the corner and you'd try to see if those logos matched up. Each of those represent the different trust frameworks that were agreed to by different players in the financial industry. And now today, you very, very rarely have to actually pay attention to any of those logos. The reason is all of these trust frameworks looked at what the others were doing and harmonized. And we think by taking a standards-based approach to both the

technologies as well as the policies and operating rules that govern these trust frameworks, we'll eventually get there over time where a credential that's used in the health community will be accepted in the financial community and be accepted when I logon to say buy something at Amazon.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Just in follow-up, that's an extremely useful answer, I took a lot of notes there. Thank you. But you raised two interesting points that I am going to change direction a tiny bit, but take advantage of the fact that I have the floor. The business model issues that you enumerated a few minutes ago, one is charge for the card, and one is to charge the relying party for the transaction. A third one that you didn't mention, but is most common obviously, is actually gain value from the aggregation of knowledge that you get from the use of the identity. I mean, that's what drives Facebook and Google and others to provide free identity services. Do you envision that that would ever become a policy issue that would address that opportunity either by saying it is allowed or not allowed or will just the market have to figure that out.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Well, there are some things though, if you read the NSTIC as it this talks about privacy, it also highlights that the government's not trying to set up, I guess what some would refer to as a nanny strategy, that would preclude people from sharing their information, a la the Facebook model, if they saw benefits out of it. I think what it does look to drive is making that a…that cannot simply be the default behavior, and NSTIC, you know, talks a lot about you need to have default behaviors at least, where the default behavior is a limited collection and transmission of information, you limit the use of individual data. Now having said that, could there be players that are out there that would embrace the model of the

ecosystem and then offer people some sort of a benefit for choosing to share that information rather than limit it. That could certainly happen in the marketplace.

We also point out, as we look to set up an accreditation process in the steering group for NSTIC providers, we expect there will be some companies that don't come to the table and continue to have their own models that work outside of what NSTIC envisions as the ecosystem. This is a non-regulatory agency, the NSTIC is just that, a strategy, it's not a policy, it's not specific law or regulation. So we imagine there will be some solutions that are outside our goals really, believing that we're going to be much better over the long term if we can improve trust online including building in privacy protections to drive as much of the market place towards that direction as possible.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Thank you.

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

Let me add a little bit to that. There were a couple of areas, primarily privacy, in the trust framework provider adoption process. We do have privacy controls and that does prohibit the sharing of information without the individual saying that you can share it. So that goes along with what Jeremy was saying. I don't want you to think that this is just kind of the wild, wild west because it certainly is not and it's more restrictive the higher that you go in the level of assurance. Also, the collection and aggregation of data. Remember that in the federal government, that is not something we want to be doing and our systems of record notices and our privacy impact assessment statements all have to say what that system is doing, what the information that is being collected, the burden to the individuals and things of that nature. So, for the federal side, we are very careful about that and we're hoping that through the steering committee we can put some of those care items in the overall ecosystem.

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

If I could add one more bit on privacy, and this is more vision than it is near term. One of the things that we are working on very hard in the cryptographic technology group at NIST is privacy enhancing cryptographic techniques. There are a number of ways that we can use cryptography to provide identity information in ways where we limit the attributes that are provided to those that are really required. On

the previous panel there was some discussion about is all of this information that's been collected and is being provided to…as a part of the transaction. Often, the information that is known by the credential provider about the user is far in excess of what is necessary to perform the transaction. So, cryptographic techniques that allow you to do things like prove you're over 21 without having to disclose your actual birthdate, those kinds of things; those are techniques that we're exploring and we hope that we'll be able to move them into more mainstream use and out of research over the next decade or so. You're certainly right that there is a complication in the business model in that sharing the smallest amount of information and collecting the smallest amount of information does not seem to be the way a lot of businesses are currently making money on the Internet. So, there are business model issues that will have to be addressed over time if those these technologies are really going to be deployed. But those are things we are looking at because we hope that privacy is not going to be an expense of this process, we want to be able to protect it and we think we can.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

And just to follow up on what Tim said is cryptographically it's quite possible to have privacy enhancing encryption. Where we've struggled so far is seeing those technologies actually take hold in the marketplace because as Tim said, not everybody wants that model. In the NSTIC pilots that we're funding, the federal funding opportunities that we published in February actually flagged the lack of a demonstrated killer business model for privacy enhancing crypto as one of the challenges we wanted bidders to address. Without saying too much, because we're in the selection process, we've got some really cool proposals around that and I think you will see some things go forward in pilots over the next year that will…may be able to actually break through that barrier.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Do you have a question?

Deven McGraw – Center for Democracy & Technology – Director

So, I'm mindful of the fact that we are already sort of eight minutes into lunch. I just want to ask one question. I don't know how many of you were here for the previous panel where the panelists and Mr. Rubin in particular described a model where sort of the organization is responsible for credentialing its individual users, but it's the organization that has the authorization to access data across the network. How does…that's been a model that we've thought through in the policy committee with previous recommendations, how does this mesh with some of the recent developments, say with the General Services Administration acknowledging certain identity providers and with the changes to 800-63-1?

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

So, nobody has come forward with that particular model to be approved, but there's no reason why it couldn't be an organizational one. But, be careful and mindful of the fact, and I think there was discussion done at the end of authorization and authentication. You're doing the authentication, the

authorization is done through relying parties. So, the people that are accessing it or asking to access information in another system, have to be authorized, right. So, just be careful of that, but there's no reason why, in my mind anyway at this point, you couldn't have an organization that was doing the identity proofing as long as they follow the rules that were laid out.

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

So, I'd like to add to that. I completely agree. 800-63 envisioned, actually, that as being one of the models. And we did put some pieces in there where we tried to acknowledge that an organization that already has that relationship, should be able to do the identity proofing more cheaply, more cost-effectively, more efficiently and there was some recognition of that in a number of ways. One of them is, as I had said before, we don't allow you to do knowledge-based authentication where you're identifying people based on public databases, but if in fact you have that relationship and it's private information that you have with your organizational members, that is something that you can leverage. And I also think that the componentizing of the process, the TF…process, would allow you more easily to say I have a credential provider that works with organizations who know their customers, and they do the identity

providing…they do the proofing and the credential provider does the credentials. That kind of thing is a very cost-effective model, I believe, over time and I think that the advances in the assessment process will make that easier to do. That said, we still haven't seen that market emerge and that's one we hope for and expect, I think over time.

Deborah Gallagher – Office of Government-wide Policy, U.S. General Services Administration

We do…that model is also there for the level 4 credential. If you think about it, the PIV and the PIV-I cards are done by organizations. There are government and nongovernment issuers, but they are done by organizations, and they identity proof their people.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

A clarifying question, so under that model where you have the organization that's doing the ID proofing, you would be expecting the organization to be following the 800-63 guidelines, is that correct.

Tim Polk – Cryptographic Technology Group, Computer Security Division, National Institute for Standards and Technology, U.S. Department of Commerce

I believe its chapter 5 or section 5 of that document. The identity…the registration section is the one that I would assume that that organization would do if you were doing that model where you're separating the identity proofing and the credential providing. Don't hold me to the section number, but it's only one

section that I'm speaking of, but yes, we would still expect them to follow 800-63.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay. I think with that, we'll adjourn for lunch and we want to still reconvene at 12:15.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, it's a quick lunch, thankfully we're located next to lots of quick places and for the members around the table who took advantage of the order ahead time, and I imagine lunch is on its way. But we'll take a break. Thank you very much for this incredibly helpful panel. Thanks for taking the time. See everybody in half an hour.

MacKenzie Robertson – Office of the National Coordinator

Can everyone please take your seats and can the panelists please come to the center table? Can everyone please take their seats?

Deven McGraw – Center for Democracy & Technology – Director

Are we missing a couple of panelists or are there a couple on the phone? Okay.

MacKenzie Robertson – Office of the National Coordinator

I would say if you want just get started and then as they come in, I know they're here, we'll just have to track them down.

Deven McGraw – Center for Democracy & Technology – Director

Fair enough. I would have to agree. This is Devon McGraw. Thanks to everyone for coming back so quickly, at least those of us who did. And thanks to our panelists who are timely here. Thankfully, the first couple of ones are here and we will switch the order, Paul, if we need to. So just again to go over the logistics for those of you who weren't here earlier. You get five minutes, the other panel had 10, it was a smaller panel in terms of the number of people. So, unfortunately we can't extend that time for you all. It

will feel very tight for you, and my apologies in advance. But hopefully during the question period, regardless of which question is asked, if there is a point that you were going to make and you didn't get a chance to make it during your five minutes, you should feel free to put it in during the question period. We'll either go in the order of the agenda or go in the order of the people who happen to be here on the panel. And we will go through, each panelist will get their five minutes first and then we'll proceed to questions from the group

We do also have some members of the working group and Tiger Team on the phone, just to let you know that they may be asking questions as well. So we'll start with Ash Evans, who is the director for corporate strategy at Verizon. Thank you very much for being with us.

Ash Evans – Verizon – Director, Corporate Strategy

Thank you Devon and my thanks to the committee members for allowing me to present today. I did put some slides up, if you could go to slide two that would be great.

Deven McGraw – Center for Democracy & Technology – Director

Clicker, there should be a clicker up there.

Ash Evans – Verizon – Director, Corporate Strategy

I've got a button. Control. These are the wrong ones, but that's fine. I'll start in this order. I am here presenting on behalf of Dr. Peter Tippett, our Chief Medical Officer and head of the division at Verizon. I represent our strategy group specifically because identity is strategic to the company. I've been focusing on identity for about 18 years. What's funny is some of the similar people are here that I testified in front of NCVHS Committee in 2004 and it's good to see the same people, but it's frustrating to see the problem hasn't gone away, right. Well, for that reason I put this slide up, and the NSTIC to us is essential. We see NSTIC important to be able to deliver a vehicle, a framework, a forum to talk about an identity ecosystem and not just healthcare, but for identity in general. The problem we're solving as an organization…at Verizon we manage identities for over 200 million users around the world, 28 different governments. Independent of our 100 million consumers, identity is a problem for us in the context of interoperability, being able to provide identity assurance, privacy controls for our consumers. We are a FICAM certified level 3 certified identity provider, so this is a strategic objective.

And I think for us, the notion of NSTIC facilitating our conversation is important and we applaud the work that Jeremy's doing. Can you go to the next slide. Yeah, I like the fact that the wrong slides were on the screen as well. We manage identity services in the context of two primary capabilities. One is what we call identity assurance services; think of those as identity proofing, credential lifecycle management, credential issuance. We manage the infrastructure for SAFE BioPharma association. So we actually issue credentials to physicians today, we're involved in the healthcare ecosystem for issuing credentials to doctors outside of SAFE. We've been participating very heavily in the NIST standards, we were responsible for altering the use of antecedent data into the NIST 800-63 standard. And the context there is the ability for us to identity proof people online based on the use of what we call antecedent data, meaning, I've already been identity proofed. We provide authentication services and authentication gateway, fully managed in the cloud as opposed to having to drop an infrastructure into a customer and we provide this to a variety of different communities, including the government, as I said earlier, 28 different agencies. I guess the point here for us is our system works to the extent that we supply services to our customers, but there is a severe lack of interoperability for us to be able to have other relying parties rely on those Identities, if we didn't issue them. And it's a problem we'd like to get solved.

From a personal point of view, I put a slide up here. On the left side you'll see a gentleman by the name of Joe McNamara, on the right side, you'll see a gentleman by the name of Quinn Evans. Quinn's my son, had leukemia. I was asked to talk about what's the real world use case where identity gets used in healthcare or doesn't, the lack thereof. The lack of an identity provided solution for Dr. McNamara at Yale and the inability for information transparency between Dana Farber where my son ended up going for his bone marrow transplant; that lack of identity assurance, that lack of identity service, proved for a lack information transparency that when he got ill, based on his bone marrow transplant, it almost killed him. When I moved from Yale to Dana Farber, I took it stack of paperwork with me. I have since worked with Yale and Dana Farber on identity solutions and they've both got independent solutions where they cannot look at information across health systems. You can share limited information through

e-mail, but they're asking for a system, an interoperable system and so from our point of view, the take-away is, we need a trusted network of identity providers, we need the ability minimally to look for world-class infrastructure certification, classification of services, whether it's for authentication or identity proofing. As a Telco, over the years, we've learned that world-class infrastructure matters. If you think about it in your own home, when the electricity goes out, the phone still works, that's the kind of infrastructure we need from our identity services point of view, especially where healthcare is regarding.

The other elements associated with privacy and trust, it's not enough for us to just look for…we've heard this notion of different types of companies being identity providers. There needs to be some oversight for the standards, for hardened standards associated with those infrastructures so that if something does go wrong, I've got Jeremy talking about the need for liability assurance. We need liability assurance otherwise it's not going to work. We have it in the context of SAFE, we have it in the context of the service level agreements that we provide as an organization, but we need to be…we need an ecosystem, a standards based ecosystem, to actually make it work more broadly across the North American public.

Deven McGraw – Center for Democracy & Technology – Director

Great, thank you very much. Next is William Braithwaite, the chief medical officer of Anakam Identity Services, it's part of Equifax.

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

Well, thanks for having me, on short notice, to come and talk in front of this committee. First of all, I'm an independent consultant, I do work for a variety of clients including Equifax. But today, I am representing Equifax as their named Chief Medical Officer for the Anakam Identity Services subset of that. I first wanted to talk just briefly about the drivers, because when we talk about identity assurance, the risk of not getting it right has three basic elements to it. There is the risk of fraud and abuse if we don't figure out who the identity is of these people. There's a risk of waste and the enablement of I hate to say the words…of simplification, because it has all kinds of other contexts for me, but the automation of what's going on in healthcare to make it more efficient and better for everyone's health; and the privacy and security risks.

So those are the drivers for making sure that this identity management lifecycle is working and is working across the whole ecosystem. This identity management lifecycle includes registering and verifying the

identities, proofing them, authenticating them, and credentialing the providers and so on. I'm not going to talk about all of that because you've all been steeped in that for some time, but I would like to talk specifically about the proofing aspect of this, because I think they are some major issues. First of all, NIST has told us that LOA 3 is what's appropriate for securing identities when you are exchanging sensitive information. The DEA disagrees, even though they quote LOA 3, they say that it's LOA 3.4. Now they tweak it a little bit. LOA 1 and 2 really aren't useful, LOA 4 is too burdensome and so we're talking about a single, relatively simple specification for LOA 3, but we have a huge range of issues of identity management in healthcare, and we don't have standards for subdividing LOA 3 into useful categories and I think we need to address that.

First of all, LOA 3 for identity proofing simply requires that you gather some demographics about the individual and then you verify their government issued ID, typically a driver's license number, and you verify a financial account number. That's not enough, you can buy a driver's licenses and equivalent IDs really cheaply. You can buy a credit card number for forty cents, a bank account number for ten bucks. The combination of the credit card number and all the contact information that goes with it is about two dollars on the open black market, and only 26 states provide drivers licenses that can be checked against, and half of those don't even update their database. So it's a really bad way of checking an individual's identity. The LOA 4, which requires a face to face, you know, you go to something like a notary public, and you show them your driver's license and they look at your face and they look at the drivers license and they sign off on it. Well that's no more reliable than the driver's license that you bought down the street.

So, we need to do something better. Now, what Equifax and other companies have done, is they have developed this concept of knowledge-based authentication. And they've developed it in a very broad and deep context. So, in addition to looking at details about the person and asking questions about, you know, what was the color of your 1970 automobile, which only you should remember because, well I'm not sure I remember, but there's the dynamics of what's going on with the account. There's the number of times that account is being attempted to be set up, there is the behavior of what's going on the Internet and on a particular account this person is trying to access. Simple things like, is the SS number that this person using from a deceased person, or did they just get it last week? These things happen, even when you're going to identify providers. So if you take a much deeper view of knowledge based authentication and do accurate questions and answers to these people to figure out who are the people, the very few number of people, that you need to do a manual research on, to figure out if they are really in fact a qualified physician or not, that is a key that I think we're going to make a lot of hay about.

So, knowledge based identity proofing can be highly successful if the data that's used is from primary data sources that's fresh and it's accurate. That is, it's got to be updated daily, it can't be monthly or every six months or so on, and it's got to be accurate. There's a lot of garbage out there and if you don't

screen it and rationalize the databases that you bring together, you're going to get garbage. It's got to clearly find the information to the claimant, it's got to be readily available to the person who's doing the identity proofing, but not to other people, which is why we use the term out of wallet questions, you don't want someone's wallet to be stolen and the information used in wallet to identify the person. That just doesn't work. You have to leverage the unpredictability of the attributes that are available when you're asking questions and they have to be guess resistant. You have to balance the accuracy of this process with the fraud potential that you are trying to go up against.

Now privacy is raised as an issue when you start to ask people personal questions like this. But in fact, these are not personal questions, these are questions like, what was the color of the car you owned in 1970? Right, they are questions to authenticate data that we already have, so it's not like you're gathering information from people. So the privacy aspect of this needs to be toned down a little bit with some education.

Deven McGraw – Center for Democracy & Technology – Director

Bill, can I ask you to try to wrap up.

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

Okay. So, I just wanted to show some brief statistics and then I'll wrap. We scanned 105 million records of Medicare providers and found that 98% of them, their credentials could be verified online; 92% of them could be processed without manual intervention with a high degree of accuracy. It was interesting that 9.6 of registered Medicare providers have criminal records. But, it turns out that most of those are things like speeding tickets and things that are not quite up to the level of worrying about fraud. But we also did a lot of screening of the organizations that these positions, which turns out to be also important. So, in conclusion, high identity assurance proofing for providers is best done remotely with knowledge-based authentication with good data. We need to work on robust standards for KBA to enable broad identity trust federation, we need to be able to use this across institutions, Verizon and Equifax need to be able to exchange that and we need to be able to do it once, do it well and then trust it, but verify by monitoring. The authentication question, we're going to leave for another time.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Thank you, Bill.

MacKenzie Robertson – Office of the National Coordinator

So Deven, Scott Howington is actually is delayed due to travel issues so he's not going to be able to attend and he won't be able to call in either. So we can get his materials and submit them to the record.

Deven McGraw – Center for Democracy & Technology – Director

Okay, thank you MacKenzie. I appreciate it. All right, we'll move along. Paul Uhrig is the Executive Vice President, Chief Administrative and Legal Officer and Chief Privacy Officer, you've got quite a number of titles there Paul, at Surescripts. Thanks for joining us.

Paul L. Uhrig - Surescripts - Executive Vice President, Chief Administrative and Legal Officer, Chief Privacy Officer

Well, thanks for having us. So, as you probably know, just for background, Surescripts is the network that's connected about 400,000 prescribers with virtually all pharmacies and payers in the nation and we handle about 20 million transactions a day. So, in e-Prescribing, I just want to talk about what happens in e-Prescribing today. The industry maintains a chain of trust from the prescriber to the EMR to the pharmacy and to the payer, largely through the contractual means. We hold the prescriber vendors responsible for ID proofing and credentialing the prescribers who transmit over the network. Prescribers today actually use various applications, depending upon their settings. So, it could be…it could be in their primary practice, in a secondary location, at a hospital or in a clinic. And in many of these locations, they actually use different applications that require different ID proofing and credentialing.

So, in the context of non-controlled e-Prescribing, today it's the EHR vendor that does some level of ID proofing and issues a username to the doctor so that they can e-Prescribe over the network. However, the level of assurance or rigor of the ID proofing does vary across EHRs, and that credential can only be used in connection with that EHR. So as you know, when the DEA issued the IFR allowing e-Prescribing of controlled substances, they focused on increased security measures and requires prescribers to undergo the assurance level 3 ID proofing in order to e-Prescribe a controlled substance. So under the IFR, EHR vendors must authenticate each prescriber using that process. So, using Dr. Smith as an example, Dr. Smith would be directed to a company like Exostar or Experian for ID proofing, which is done remotely, or otherwise. Once the ID of Dr. Smith is confirmed, Exostar using them as an example, would complete the authentication process, issuing to Dr. Smith a two-factor credential or electronic identity. But Dr. Smith still can't use that identity across other applications for other purposes and may not even be able to use it for a different e-Prescribing application that he or she uses.

So while the digital identity may be secure, it is just not interoperable. So this is where, in our view, the NSTIC vision comes into play and I just want to talk a little bit how we see that working in our environment. You've heard about the harmonized standards and NIST 800-63 and Kantara, so I won't speak to that. But one example of how the NIST concepts can be implemented is something that we call a trust broker, someone who could essentially have access to a provider's credential that's already been issued. So, in my example, Dr. Smith has already been credentialed. If another EHR wants to allow Dr. Smith access, Dr. Smith would point that EHR to the trust broker and would be able to verify the identity of Dr. Smith and now that other EHR could rely upon the ID proofing and credentialing that's already occurred so that Dr. Smith can now use that same credential on two different EHRs. This would obviously reduce the administrative burden imposed on Dr. Smith as well as others.

We also see a scenario where this could be used not only for e-Prescribing, but for other healthcare applications or either non-healthcare applications. So, we proposed a pilot that would test using and leveraging EPCS to be able to access other portals for communications, clinical communications, to be able to communicate with a state Board of Pharmacy for recording requirements, filing audit documents with CMS. And one can even envision a scenario where these credentials are used to get into the hospital parking lot or pay for lunch at the hospital dining room. So, we believe this is a real possibility that we certainly have proposed a pilot with ONC and NIST. So a lot of this is obviously being driven by the federal government; what can the government do in our view; one, support pilots to test the models, emphasize standards and collaboration, enable easier compliance to single identity frameworks and then provide recommendations on assurance levels that can act as a safe harbor. So, in conclusion, we believe that with the introduction of EPCS and the identity standards by NIST and Kantara, NIST can provide a real live proving ground for the NSTIC vision, while meeting the requirements of HIPAA and create a strong digital identity management marketplace. Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Thank you very much, Paul. Next, we'll turn to Dr. Thomas Sullivan who is the chief privacy officer and chief strategic officer for DrFirst.

Thomas E. Sullivan – DrFirst – Chief Privacy Officer, Chief Strategic Officer

Thank you. Do you advance the slides or do I do it with this.

Deven McGraw – Center for Democracy & Technology – Director

Whichever you prefer? But you can do it with that clicker.

Thomas E. Sullivan – DrFirst – Chief Privacy Officer, Chief Strategic Officer

Okay, good. Thank you. I'll go through these very quickly because I know the time is short. There's just a little identification of who we are, DrFirst, a small E-Prescribing company, oh you can't see that background. I'll just say we're the…we have some experience in this area, we're the first company to begin an EPCS pilot in the United States under a special DEA waiver. It was a three-year program in Berkshire County, Massachusetts and it was funded by AHRQ. Thank you AHRQ, giving that money to the Massachusetts Department of Public Health. We're also the first company to send out outpatient electronic prescriptions for controlled substances and this was prior to the DEA IFR that was published in June 2010. But we participated with them in helping to find at least that interim final rule.

We've more recently…what did I do?

Deven McGraw – Center for Democracy & Technology – Director

Went backwards.

Thomas E. Sullivan – DrFirst – Chief Privacy Officer, Chief Strategic Officer

Okay, there we go. We partnered with Symantec and Experian to meet the NIST level 800-63-1 and this is our product EPCS gold. And it's highly leveragable, the front end is customizable, the back end decision processing is completed by Experian and it sits outside the normal e-Prescribing workflow. So, let me give you a little bit more of a narrative, which was also printed in the manuals that were handed out. My personal background, I'm a cardiologist from Massachusetts with about 40 years of direct patient care, and over the past eight years I've been working for DrFirst. And recently, at a little conference in Arizona, talking about our experience with identity proofing, after the conference, I was invited to this small White House colloquium where I first learned about, I'll call it NSTIC. I don't know if it's NSTIC, but NSTIC. And I was unaware of NSTIC at that point, but after the colloquium, I really became enthusiastically supportive of the goals and objectives, particularly in health care where the redundancy and inefficiency is absolutely legendary. You've heard from some of the prior panels about that, so NSTIC could clearly make a difference. Today I'd like to give you a little bit of our experience, preliminary example of where we can share trusted identities and make other recommendations.

Now, my experience in this area, not unlike other physicians, it has some unique elements and some common elements. As a past president of the Massachusetts Medical Society, the oldest Medical Society in the country, I am aware that in 1781 we did the identity proofing and for about 100 years that's what we did. Just after the Civil War, we petitioned the state legislature to create a State Department of Public Health and it's the oldest one in the country, the oldest state one, and they took over the identity proofing and the licensing. DrFirst, we participated in this three year project that I've already told you about in western Massachusetts and the results have been published by Brandeis, so we could share our findings with everyone. With our corporate partners, Symantec and Experian, we've been rolling out the identity proofing in a hard token, a one-time password device for the past several months. Since the current availability of retail pharmacies that can accept EPCS and the variability of different statutes in each and

every state are limiting factors. We have seen some reluctance to become early adopters on the part of the physician community. Approximately 12 states still do not allow EPCS, despite the presence of the IFR, although I think you heard earlier, just a couple of weeks ago, the legislature in New York passed a law mandating EPCS, I think around 2014.

In addition to that reluctance, many physicians are hesitant to release financial credit card information over the telephone to satisfy at least the current interpretation of NIST 800-63. And we've had some face-to-face meetings with NIST to offer some acceptable alternatives to certain financial instruments and credit cards. We've had some verbal indications, I don't know if Deb is still here or not, but that these might be acceptable, but we're still waiting for a written confirmation to again, make this easier.

So, despite the somewhat slower uptake than we initially expected, at least we're assured and pleased that once the physician and prescriber is identity proofed and has been adequately authenticated, the controlled substances are actually being sent out in several states around the country. So, this is real-world proof that we have that the system is actually working as it was originally designed.

Now, as a practical example of how NSTIC might work, I was recently given verbal assurance by the Massachusetts Department of Public Health, the controlled substance division that they would

strongly consider using the NIST IDP process to eliminate their current procedure that they require to access the state prescription drug monitoring program. Some of you may know that many states have had these so-called PMPs in place and they've had sort of limited and variable success in helping to manage the controlled substance abuse and fraud, and I know my time is up, but I am just saying that sharing trusted identities could make a real difference. I don't believe that this level of assurance is necessary to access these PMPs, but there could be some delegation. We've been talking about administrative simplification for many years, even prior to HIPAA, and although, there's progress, more can be done.

Finally, I'll just say physicians and other clinicians are among the most highly credentialed and authenticated professionals in our society. It's just going crazy. There's a lot of redundancy, unnecessary delays and excess expenses. And, it's not just the states, it's every single health plan, it's the hospitals, it's the privileging, so forth and so on. It is getting more complex daily, it cries out for a better solution. Final statement, cost effective care and the elimination of redundancy need to be the hallmarks of 21st century medicine. And I'll put it another way, the first rule of medicine often traditionally recommended for physicians is, prima non nocere, first do no harm. So I would add Dr. Sullivan's second rule, secundo propara ne me, second, don't slow me down…(laughter). So, we'll be happy to answer questions. Thank you.

Deven McGraw – Center for Democracy & Technology – Director

You got a great response out of that last one. All right, our last panelist is Steve Kirsch who is the Founder and Chief Technology Officer of OneID.

Steve Kirsch - OneID - Founder and Chief Technology Officer

Okay. I'm going to start by agreeing with Farzad that the FICAM approved identity…that what we have now is not good enough. The FICAM approved identity providers that Jeremy suggested, I don't think are good enough either. The top CIOs in the government met, they agreed that ICAM is the number one problem to be solved in 2012. We have issues with OpenID where even the top providers, aren't allowing login with anyone else's OpenID to their site. And the list goes on, security issues and so forth and SAML, I think, is even worse. So, that's why I started OneID about a year ago. And it's basically a high

assurance general purpose digital identity ecosystem, designed to eliminate all use of shared secrets including usernames and passwords. It was designed from scratch to exceed all of the NSTIC requirements, so it was actually designed after NSTIC.

And so we took all of those things into account in designing the architecture of this; easy to use, easy to deploy, all the NSTIC requirements, uses people's devices that they already have, so that you don't have to supply a token and provision that.. I have security on demand so that relying party of the user can set the level assurance to whatever they want. It supports multifactor and out of band to LOA 4 user centric, preserves privacy. The preservation of privacy is guaranteed by the architecture and not by policy. So, you don't have to have people pledge to preserve privacy, it's actually guaranteed by the architecture. And it's multi-provider so that all these guys can interoperate with the same standards. There are twenty people in the company, we've got seven million in funding, and we have over 375 RP's today, pre-launch.

So, what is does is essentially authentication, it also does authorization, digital claim storage and assertion. So you can…it provides a framework so that you can ID proof just once for all the RP's and then reference that. And it also allows proving with privacy so you can prove that you're 21 without disclosing your date of birth or name or identity and here's an associated biometric with that. So, you can do all these things in a private way. You also have secure attributes storage and sharing and secure information storage.

And so the way that it works, basically is one digital identity for all uses. You prove to your device that you are you, and you can do that with an out of band device as well. And then your device will digitally assert your identity using public ecrypto, we use NSA Suite B, ECC P-256 for all of PRPs. And there's a very complicated protocol for the signature flow where it goes to your device, your device then talks to a repository in the sky which then, if it's appropriate either by your suggestion or by the RP's request, will hit an out of band device which then performs a third digital signature and so the three digital signatures then are gathered at an RP so you have end to end security on transactions, not just login but also for authorization. It preserves privacy because the users in the center of that transaction, so they can't disclose any information at all to any relying party without the users express consent and involvement.

So, its other unique features about OneID's general-purpose, its guaranteed privacy, identities are only asserted or is shared with express consent, guaranteed by the architecture. We will have mass adoption, it is free. We have leading retailers who love it and want to deploy it. It speeds up transactions, as Thomas wanted to do, rather than increasing friction. User-friendly, have it your way, level of authentication. Mass breaches are impossible, like you know the LinkedIn breach where you had all these identities…that's impossible to do in this architecture, because it's being held at user endpoint devices. Very quickly, how we would do physician authentication and authorization is that OneID actually mimics real life, so you can say hi, I'm Dr. Fred Smith, here's my license and here's my signature. The relying party then can verify that signature, verify the cert, verify the cert hasn't been revoked; very simple, very simply.

You can issue physician credentials as a simply as clicking on a link at a website, so you go to the Medical Board of California, click add the license cert to my OneID it's done, and you can go and prescribe and as far as acceptance of those prescriptions, then when you go to your EMR system and hit submit prescription, that can be digitally signed by your EMR system and it can be verified by everyone along the chain. And so you have end to end…not only end to end security but security as the transaction's going through the system.

And so you can also use the same system for patients so they can be authenticated as well. I know that's not a part of this hearing, but it's nice to have the same system that's being used by doctors and patients. And you can provision a user in about two minutes. And that's with an out of band two-factor. So it's not just two-factor, but it's really important that the two-factor be out of band so it's not like an RSA SecurID which is like writing a blank check, even though it's two-factor. And finally, a demo is available for all of this, I mean it can show you how we can add a medical license to your identity, how you can assert that license at a different RP and I have, in the written materials, there's some more on suggested IdP requirements and we're very open to collaborating on the design. This would be an ideal point because we have not released it publicly, so if we're going to change protocols and add things, this would be a great time to talk to us.

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. Thank you very much. We'll move into the question period and ask folks to hold up their cards. Walter, you've already got yours up, you want to go ahead.

Walter Suarez, MD, MPH – Kaiser Permanente

Sure, thank you. This is Walter Suarez. Great overview and now we're going to get down to the details, so that's really nice to see how some of the private sector efforts are working. The question I have is about…so we have a large organizations or even smaller organizations that issue their own IDs to whatever level they have for use internally, mostly by the employees, whether it's a physician, a nurse or an administrator or receptionist. I was trying to understand how do you see that playing into the type of external certification and external IDs that you'll issue, because if I am an employee of X organization, that organization is going to issue me whatever they have today, right, I mean it could be a level 3 certificate or some ID that I could use to authenticate myself to the internal system. But then if I'm going to go outside of one organization to log into another organization to access health information, for example, whether I am a physician or nurse or whomever, then I'm going to have to rely on one of these external certificates that are being issued perhaps by one of the organizations, you know, the kind of

certificate I do issue. So, how does this play when it is in those two types of situations, an internal organization issuing IDs and certificates to their employees, and externally some other entity, Verizon or OneID issuing IDs to the same person so they can access externally others. Or, is the idea to ultimately replace all these and have just an entity, like Mayo or Kaiser or someone else, just relying on the same certificate that is issued to the employee for internal use that that employee can use externally? How does that play?

Deven McGraw – Center for Democracy & Technology – Director

(indiscernible)…to the panel to…

Walter Suarez, MD, MPH – Kaiser Permanente

To the panel, yes.

Deven McGraw – Center for Democracy & Technology – Director

Okay, Steve?

Steve Kirsch – OneID – Founder and Chief Technology Officer

So, in our case, we hope that people will…the organization will provision our identities, a OneID identity for use internally and it was designed so that it was so general-purpose that it could be used for enterprise apps as well as externally even, for their consumer use, so that a person would be able to use that same identity, because people don't want to have to manage…I mean, the whole thing that we got from consumers is that they're sick and tired of managing all of these identities. And so what we do is provide people a way out, give people an identity that can be used in all of these situations, that's in fact stronger and easier to manage than those internal identities that they are using now. And at lower-cost, too. And so, it'll take a while to get there, but the point is that it's just a better choice to outsource the identity because a hospital shouldn't be in the business of having to become identity management.

Walter Suarez, MD, MPH – Kaiser Permanente

Any others?

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

It sounds like evolution, if you believe in that, survival of the fittest or maybe the cheapest. Eventually, larger organizations will find that it's actually cheaper and safer for them to rely on larger external organizations for identity proofing and certification and that sort of thing, I think.

Ash Evans – Verizon – Director, Corporate Strategy

FICAM, the notion of FICAM and NSTIC, is to answer that very question, right. The notion that we have trusted certified authentication or trusted identity providers that we can rely on, as opposed to saying I'm going to try and federate all the identities in this room, which we know doesn't work, won't scale. So I think minimally if you have an identity management system that you built for internal purposes, the objective of mapping to a trust scheme that we all agree to, or one of many, I mean, you can have more than one, is a minimum requirement. Otherwise, we're still having the same problem, we can't speak 50 different languages at the same time. So, we need a minimum set of standards and minimum set of requirements we can all adhere to, otherwise, we're going to have mass hysteria, confusion and we're not going to solve the problem.

That's why I think from a Verizon point of view, we like NSTIC, creating a forum where we can agree on some of these standards. NIST sets them, how we implement them and how we think differently about things like identity proofing, location-based authentication, meaning implementing different mechanisms. It's not about my identity or his identity, it's about how many different mechanisms we can invoke into the system to make sure that the person doesn't really need one form factor, they can choose. The system doesn't really rely on just an assertion from Verizon because we are the identity provider. We can rely on other mechanisms, other network-based capabilities that exist today which is not using them.

Deven McGraw – Center for Democracy & Technology – Director

Paul and then Tom?

Paul L. Uhrig – Executive Vice President, Chief Administrative and Legal Officer, Chief Privacy Officer, Surescripts

Right, so agreeing and not repeating with everything else that has been said, using the DEA example, right, so we see the world where 400,000 doctors at some point will have been credentialed pursuant to that level of assurance 3, which is a pretty high level of assurance. And that should be able to be relied on

by other relying parties, eliminating the need for all the multiple credentials that are needed today. So, reaching that standard is very much, I think, the NIST vision.

Thomas E. Sullivan – DrFirst – Chief Privacy Officer, Chief Strategic Officer

Just addressing that issue, I have to say this is where it's so important that the government be involved, not just the federal government, but also the state-level governments. And in my state, our HIE is being formed right now and we have hopefully an advantage. I think most of you know John Halamka, who's helping to head up our HIE and some of the standards that are being developed. But the liability in these trusted identities and sharing for healthcare I think is far greater, at least from my experience at Partners Healthcare in Boston, the liability is far greater than the banks exchanging ATM stuff and in all honesty, I know that everybody touts that as a success and says why can't healthcare do what the ATMs in the banks have. Well for me, it's only about money with them and I think we're concerned about the liability. One other thing, I have a colleague here, Peter Kaufman from DrFirst who also is very much involved with us. And if I could invite him to answer some of these questions, too, that would be great.

Deven McGraw – Center for Democracy & Technology – Director

Yes, if there's a question that comes up that you can't answer and you want someone from your company to answer, that's fine, but I think we, again, given time, we want to be careful about how we divide it up and make sure that everybody has an opportunity. So, thanks, Walter.

Deven McGraw – Center for Democracy & Technology – Director

Dave, I saw your card up next and then Wes and then David.

David Cassel – EPIC Systems Corporation

This is primarily for Steve Kirsch. From your written material, it sounded like you've developed your own API that's specific to your solution and that you…you made comments here and in the materials about SAML not being sufficient. I would contest your statement, by the way, that vendors will SAML, but, in any case, it sounds like you perceive a need for…you perceive a need for a standard that's there, if in fact you developed your own API. Do you have suggestions for existing standards that are out there, if you don't think SAML is the answer, or do you think that there's a completely new standard that's needed?

Steve Kirsch – OneID – Founder and Chief Technology Officer

Um, yeah. I mean the reason that we developed this standard…the APIs that we did is because the existing standards never contemplated user-centric identity systems and that's where things are going, that's the way things have to go. And there are not even…like OpenID is not PK-based at all because they wanted to be compatible with the systems that were out there. And so it didn't mandate use of PK so, and even then, when it uses it, then it's using reliance on an IDP and so it has very centralized IDP model as does SAML. So, all of these systems that were designed, and we can talk for a long time about the standards process and what results at the end point of the standards process, because you look at SAML and there's like one guy in the world who's the expert of it and can actually have a definitive implementation of SAML. And the other people are always trying to be…it's just so complex.

And the second thing, is that it didn't contemplate a world where we had to change the architecture. And so when we looked at existing architecture, as we said, this doesn't work and people keep doing the same thing over and over again, expecting a different result. We had to think completely differently, and so we couldn't use any of those existing standards. Now could we go and shoehorn this into OpenID, well, OpenID's this moving target, it keeps changing and they keep change…oh, today it does this and tomorrow it does that. So, I guess we couldn't, but OpenID really was set up to be this front end to existing IDP systems…because there's IDP centric systems and has this IDP centric model whereas we are a user centric model. And so, it's questionable whether that's a good idea. And so what we'd rather do is say hey, here's the user centric, new way to do this; let's keep the protocols really, really simple and make it a standard as opposed to trying to create this one standard that tries to solve everything for everyone and just becomes a real mess for everyone when they do that.

Deven McGraw – Center for Democracy & Technology – Director

Okay, go ahead, Wes, and then David.

Wes Rishel – Gartner, Incorporated

Steve, you made a comment that a lot of the security from your approach comes because the real bit of information that authenticates the user is on their personal device. What is the procedure if they lose their personal device?

Steve Kirsch – OneID – Founder and Chief Technology Officer

There are a couple different alternatives. For example, my identity is put on several different devices. So I have many devices that I have. I also have a provision on my wife's device, so she can approve my transactions but not generate transactions. So, we split your identity, and we put it on…your identity can be put on many devices, and the key to your identity is also split among several devices. And so if you lose a device, you can use your existing devices…the approval from your existing devices to re-provision a new device. And so we had to invent a new secure protocol to do a transfer of cryptographic secrets from one device to another device via a cloud that acts as a pairing server. But there are actually two pairing servers and so we had to create a cryptographically secure way to do that, in such a way that if the pairing server that transferred the secret was compromised, that they still couldn't learn the secrets of the secrets that are being compromised…I'm sorry the secrets that are being transferred.

So the point is that you needed a way to do end to end, secure transfer of secrets from device A to device B, in a way that's user-friendly. And so the way that we do this, in practice, is you that take your cell phone and you take a picture of the device that you want to authenticate, then use with your identity, so that the secrets can be transferred there. And so it's as simple as taking a picture of the new device that you want to securely transfer your cryptographic secrets from device A to device B. And if you don't do it with the cell phone, if you don't have a cell phone, you can use a numeric pairing code technique. So it's very similar to how Netflix provisions; so what happens is you type your password on the new device, it gives you a number, you enter the number on your old device and that, because of the way the crypto is designed, it can securely transfer the secrets from one device to the new device via a third device and even if a third device is compromised, the crypto secrets are not compromised. It's very cool crypto.

Wes Rishel – Gartner, Incorporated

Okay. Bill, you talked very briefly at the end of your talk about screening organizations rather screening individuals. Is the process essentially the same, that is, it relies on known information or is it a different approach? How does that happen?

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

The process of ID proofing organizations is different in the sense that the public records that are available about organizations include only include a few of the individuals associated with that organization, so you have to ID proof the individual that has a record of being associated with the entity. And then using that relationship that's been established, move forward with authentication. It's a trusted agent approach.

Wes Rishel – Gartner, Incorporated

Okay. This is in reply to something Tom said, but it's not meant to start a debate, I just think it just has to be said. In other words, I get the prerogative to say it. We talk a lot about the success of the transaction card industry, the financial industry. We kind of forget that it took 30 years, but we talk about it. And, at the same time, we talk about the fact there's no way to put a value on the breach of medical information. If there were no way to put a value on the breach of financial information, we wouldn't be talking about the success of the credit card industry. Someone said today, we don't want a…I can't paraphrase it right now, but the point was not that we could avoid condemning, but we can understand and understand how to share it as opposed to having it be this uncapable amount, and I just think combining that with the comment earlier today about if you get two people that want to do things together, you find a way. The thing that prevents them from wanting…one of the things that prevents them from wanting to do things together is uncapable risk. So, I think we have to find some way to quantify healthcare risk if we really expect to make much progress in this area.

Deven McGraw – Center for Democracy & Technology – Director

Thanks Wes. David McCallie?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, thank you, David McCallie here. I have a bunch of questions, but I'll pick one and maybe we can cycle back around it and multitask. To start with, Dr. Braithwaite, about knowledge-based authentication, there's kind of an unstated assumption that the knowledge-based system is capable of understanding who the person is that they are authenticating well enough to match the right questions to that person. And my experience is that that fails, and I have a couple recent examples in my own personal experience. One was, I did a bank transfer that required a telephone call authorization in order for the transfer to go through and the first three questions I flunked, and I was really getting nervous. A, because it would be a problem if the transfer didn't go through and B, because why am I not who I think I am. And finally I got to the last question, it was one last strike and she said, what color is your pickup truck? And I realized at that point that they were authenticated my father. And the good news was, I knew what color the truck was and that was sufficient for the transaction to go through, but it's hardly good enough for healthcare. So my question is, how can you make knowledge-based authentication work when you have to somehow have already authenticated who you're authenticating?

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

I think that's a good question. And an approach that seems to work well, particularly in cases like that, is that if you gather the data from many, many sources about individuals and you form like a golden electronic identity of individuals ahead of time, so that you would differentiate the information about you from the information about your father. When it comes to asking the questions, you can look to see what questions would differentiate those two identities with the same name or something that's very close right up front. It also works when you are trying to match electronic records on patients for example. The method of taking two records from two places that identify patients differently, and matching them or trying to match them, is a lot easier if you take the first record and match it against sort of a golden electronic identity of a person and then try and match the second one, and if they come up to be the same person, it's much more accurate than trying to do that with the limited information available on those two records.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

In follow-up, that golden electronic identity, if you have that and have sufficient confidence that it's right, why are we not using that as our identity? In other words, you have to kind of solve the problem before you can proof anybody into the solution of the problem and something doesn't feel right about that.

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

We'll have to talk later about what you don't think feels right about that, but yeah, that is the approach that Equifax is taking to providing secure identities using knowledge-based questions.

Deven McGraw – Center for Democracy & Technology – Director

So John's card was up first and then you Gayle.

John Houston – University of Pittsburgh Medical Center

Thank you. One point back to I think something Wes said, and somebody on the panel says, well the basis for identity proofing in banking is still if you want to open an account, you have to show up at the bank, it isn't…oh yes you do, but to initially open up an account, so I just went through that with

my daughter, and they required all sorts of identification and credit cards, you name it, she had to do it. So, I think we shouldn't use banking as a good example because the initial intake from the banks is actually showing up somewhere in person. But to my actual real question to the group is one, I think that there's been a lot of talk about physicians and earlier discussion, I think for this environment to work, we have to look at everybody who's involved in the process of providing healthcare, whether it be staff in the hospital or a physician's office or otherwise. And we also have to envision a very high-volume, very robust environment and I guess the concern that I have, at least in some of what I heard this afternoon, was are we able to sustain the volumes and are we able to extend it to all of those other individuals that either need to independently access information or access information or actually authorize services on behalf of, for instance a physician. You know, if a physician provides an order to somebody and that individual actually submits the order, how are we going to…how do solutions work to satisfy those requirements?

Ash Evans – Verizon – Director, Corporate Strategy

From an identity perspective, we do it now right, so when you buy a phone, and it doesn't have to be face-to-face, we identity proof people. We are being identity proofed on a daily basis through a variety of different mechanisms. The ability for us to bind different things to you, the device, your IP address, your vehicle, the keys to your house, those mechanisms exist. What's missing is the interoperability of those mechanisms and use of those mechanisms relevant to the specific context with which we're having a transaction. Somebody asked a question earlier about…well David actually…knowledge-based. If we knew that your phone was in Chicago and your IP address was in Chicago, but perhaps your father lives in San Francisco, were not going to authenticate you from that perspective, right? So I think the utilities of that…the conversation hasn't been had and that's why we're promoting NSTIC in the context of getting a form together to say, look, what are those different capabilities, what are those different mechanisms.

I think the other point of view, relevant from a…it is going to require a world-class infrastructure. I think we need to face that, I think the notion that we're going to peck away at it around the seams versus really solve the problem, and there are experiences or examples. Banks, although the transactions aren't identical, it's a world-class infrastructure and it works; it takes hard core 24/7/365 support. Those are things we should embrace, they're not things we should walk away from. The transactional aspects, we're entering a new forum in the context of cloud computing and basically now companies are outsourcing more of their transactional systems than they ever have, so the ability from a transactional point of view is there also. As I was saying earlier, in 2004 we had this exact same conversation, the difference was, there wasn't a forum to actually solve the problem, and the capabilities that we're invoking today are more advanced than yesterday.

My bank is able to ask me not a shared secret, meaning what's my favorite dogs name, but which of the following flights did it take yesterday? That's a really hard thing to spoof. Right, so those are the kinds of transactional systems we should be invoking versus looking to the traditional elements or the traditional authentication mechanisms.

Paul L. Uhrig – Executive Vice President, Chief Administrative and Legal Officer, Chief Privacy Officer, Surescripts

I agree and I would add that part of the question that you're asking goes well beyond the identity of the individuals involved, it revolves the relationship network that needs to be established between them, and the authorizations that flows through that network which we aren't talking about today. It's a major issue, I think, as part of this eco-structure that we are building, that we have to think about that as the next step.

Deven McGraw – Center for Democracy & Technology – Director

Steve.

Steve Kirsch – OneID – Founder and Chief Technology Officer

So, I think you're asking a great question. I don't have the answer, but I know doctors will frequently say to their assistant, I think one of the other panelists had put this in their materials, that doctors don't have time to write the prescription themselves, they're going to give it to their assistant to go and write their prescriptions for them, enter it into the EMR system and so forth. And so, I think we have to decide how we're going to handle that. But an identity system that can handle it both ways; so for example, our identity system allows you to give someone else your identity, so that they can act as you and you can then observe what they did with your identity, so you can double check on them. Or you can give them your identity to initiate and then you just hit approve, so that the doctor could say, hey I'll give you initiation ability, but I'll make sure that the final thing was approved, so he just looks at the final thing, whereas the assistant just enters in the prescription itself. And so that's one way to do it.

The other way to do it is for the physician to say, hey, I'm delegating authority, here is a signed certificate signed by the physician, that has been stored in the assistants record so that when the assistant signs it, they can include the digital certification from the doctor. And then if that's accepted, then that's another way to do that. But I think the more practical way to do that and still have the assurance is to delegate the assistant the ability to initiate the transaction, whereas the doctor keeps the final approval, which minimizes the physician's time, but still gives accountability that the physician is the one who ultimately is responsible for that prescription, even though they didn't do the work of actually entering it.

Wes Rishel – Gartner, Incorporated

So the provider agent, as we call them, already does this many, many thousands of times with prescriptions and if I'm not mistaken, NCPDP script 10.6 has a field, and it's especially true for EPCS, you want to make sure that both names go through. Peter, do you…does NCPDP 10.6 have those two fields.

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services

The two fields are actually eight. There is a provider agent field in eight, although it's used in different ways by different applications, but it's meant to be who is the agent. I think Steve subtly corrected himself with what he just said. The issue is not that somebody is using your credential or using your identity, it's that they are acting as an agent for you and they have their own identity and their own identity is identity proofed and secure, and it's logged and audited, and they are an agent for the physician who is then countersigning later, saying that yes, this agent did things properly. But the important point is that they do not take on your identity, what they're doing is acting as an agent for your identity and have permission for that.

Deven McGraw – Center for Democracy & Technology – Director

Okay, so Gayle, you're next. We are…we're borrowing a little bit of time from the next panel, because it's only got two presenters on it, but we are creeping up towards the end. But, go ahead Gayle.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Thank you. This has just been fascinating and to see the real-world examples out there of companies actually doing what we want to make happen to a very large degree across the country, is just phenomenal. And the thousand flowers blooming out there, we have four or five, five of them here right now, I just think it's absolutely fantastic. My questions, and in a very practical vein as we go down the whole track of this is, what is this all going to cost to the individual provider. I'm a small doc on the block, I've got maybe four practitioners in the practice, what is…as I'm getting into this whole world, what's it going to cost me at the end of the day to have this kind of system in place? Am I going to be able to afford it? Am I going to be…what are you…give me some ideas as to what this is all going to cost at the end of the day.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

…sorry, Farzad. So if I could just add, if you could also answer, what is the cost today and what would it cost in two years from now?

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Exactly, thank you Farzad.

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

I'll go first.

Deven McGraw – Center for Democracy & Technology – Director

Somebody had to do it.

William R. Braithwaite – Anakam Identity Services, Equifax – Chief Medical Officer

Yeah, somebody has to do it and maybe I'm more independent than most. So, I'll tell you. All you have to do is look at the GSA schedule to see what the trend is. The trend over the last two years has gone from five dollars per identity proofing to fifty cents per identity proofing, and it's one of these curves that's going to come close to zero pretty soon. So part of that has to do with the volume, and in some companies, it is…we're going to open it up to the world and get as much volume as we can; others are trying to sell high-volume identity proofing to large federal agencies, and if they can get somebody to…like the SSA to pop in for 300 million identity proofing's, then for everybody else it will be close to zero, because the work will already have been done. So, I think it's coming down fast and it's going to go faster.

Ash Evans – Verizon – Director, Corporate Strategy

Dr. Tippett went on record in November 2011 to say Verizon would give physicians level 3 credentials, meaning we're not making money, our business model is not to make money by issuing credentials to physicians or to providers. It's likely that you'll see us be able to issue high assurance identities to consumers based on the existing services that we offer to you today. It's a question of where you can use those identities and what's the value. Somebody else asked, I think it was David and Wes, where is the opportunity, how we are making money in this service.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Are you charging then per click or…that you're working off, you know the hospital that I'm going to access that record for, is it a per click charge and how much is it going to cost that hospital?

Ash Evans – Verizon – Director, Corporate Strategy

So there are over…and today they have authentication systems in place, they have privacy management systems in place, and so we deliver those services of the company to them today as an enterprise, that's part of our traditional business model. I think what we are missing is the future, there isn't a privacy enabler today. You don't have the ability to say, stop using my information without my authorization. And so from our point of view, there needs to be one and that's one of the conversations we're having with NSTIC. Who will be the privacy enabler to allow you to be able to say only you can control how someone uses your attributes, your personal information and that would include your personas, whether it be your employee persona in the context of being a physician, or a patient or an employee or an anonymous persona. And so we think there is an opportunity for attribute exchange verification, meaning being able to verify claims, I am over 21, I'm a father, I'm an employee, and I'm a licensed physician, as an example. So there are business models there where we will…where companies will make money based on the attributes associated with an identity. The primary business models we're seeing with regards to identity assurance today are, we charge for a credential perhaps, depending on the level of assurance, depending on volume, we charge to manage the infrastructure for the organization that may need to have it managed, meaning outsourcing those capabilities as opposed to building them themselves and building them themselves and we do see an opportunity to charge based on the volume based clicks, much the same way we as we do for telephone calls today.

All three, in fact four of those models, we'll see evolve over the course of the next few years. Our goal though is to ensure these identity credentials are pennies on the dollar. The question is what's the value to the person to manage that information to have a certified trusted identity provider manage that information and make it usable, ubiquitous by all the relying parties they want to do business with, or interacting with. And the entities that are going to rely on the identity, the assertion Ash is Ash, he works for Verizon and has a high assurance of my identity, the veracity or at least the risk associated with being wrong, will predict or predicate the cost the companies are willing to pay to rely on that identity, not independently, but it'll be part of the problem that Wes was talking about earlier. So, a high assurance transaction in the case of David, who wanted to make a financial transfer, where there's risk that David's not David, and we need a higher level of assurance, the entity, the bank in this case, is going to pay a little bit more than they would if David was going to buy a pair of flip flops.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead Tom.

Thomas E. Sullivan – DrFirst – Chief Privacy Officer, Chief Strategic Officer

And so, I agree with the prior panelists. Our business model is variable, taking a page from the Medicare payment reform that is offering bundled payments now, we have bundled services. So the identity proofing hopefully will be pennies, but other services that are associated with that will be the revenue generators. We have a number of different models that are, some transaction-based, some just upfront if you want to just do an independent, and I think that's the way we see the industry evolving, with multiple business models.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead Steve.

Steve Kirsch – OneID – Founder and Chief Technology Officer

So quickly, agreeing with the other panelists, I think there'll be a lot of business models. It's kind of like asking, well what will the cost be for a credit card. Well I can get some American Express cards for zero annual fee and I can get other American Express cards for $450 a year annual fee. They offer different benefits, but there's going to be a range of solutions and consumers are going to be allowed, and providers and so forth, they're going to be allowed to pick which solution fits them the best. But I think the answer in general is, it's going to be very, very affordable; it can range from free…like PayPal makes billions of dollars a year by giving away sort of free use of money transfers and so forth, because they make it in other ways. Cruise ships sort of give you the cruise for free and they have a captive audience, they monetize the audience. Right, so you have all these creative ways that, for example, we could give our identities away for free and monetize it in some other way in your transactions and so forth. So, you're going to see a variety of different business models, but it'll be very, very affordable, in the order of dollars per user per year kind of thing, like ten dollars a user per year, in that range, I think.

Deven McGraw – Center for Democracy & Technology – Director

So, we're already fifteen minutes past when the next panel was supposed to start. So, Joy, you were the only one who hadn't had a chance to ask a question already, who had a card up, so, but it's wasn't clear to me whether you put in down due to time or…

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

I put it down due to time and I'm not sure the answers would be short here. But I will throw the question on the table, at least for thought, which is, what is the next logical steps from the perspective of the people who are actually in the field now? And, given our short time, if you could send us e-mails or something, I guess that would be the way to get your response after you've thought about it a little bit; unless you can do it in 30 seconds, according to Deven.

Ash Evans – Verizon – Director, Corporate Strategy

Encourage more participation in NSTIC would be the first thing. More participation, more companies involved in the table, more people basically sharing in the development of the standards and the process.

Steve Kirsch – OneID – Founder and Chief Technology Officer

I would agree, if the companies just sitting around the table here and a number of others could just start talking with one another with the blessing of NSTIC, I think those are the next steps.

Thomas E. Sullivan – DrFirst – Chief Privacy Officer, Chief Strategic Officer

I think pilots that are not super aggressive that involve a few number of people who can start to demonstrate what you're trying to achieve are very valuable and rather than trying to have it very big and grandiose and trying to involve six relying parties and so forth, is to keep it relatively small, pick a few vendors, put together a pilot. Don't try to make it too aggressive, start there, see how that works and then go to the next step, right, take a series of small steps as opposed to try to solve all the world's problems in just one big step.

Deven McGraw – Center for Democracy & Technology – Director

That's not what NSTIC was for, I'm so confused. Paul, did you want to add anything before we close? Okay.

(Indiscernible)

M

We will start with CMS next.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, yeah. I'm sorry that we didn't have a chance to do another round for those folks who had questions. I want to thank very much the panelists for taking time out of their busy schedules to enlighten us today, we very much appreciate it. Folks, this isn't actually a break. It's just a panel transition, so if we can ask for our presenters…presenter in our fourth panel to please take a seat and for folks to take any conversations off-line so we can get started. Thanks a lot Tony. You have the benefit of being…you're the only one who's physically here, so,..

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Can you hear me?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, we can.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Ladies and gentleman, distinguished guests, etcetera.

Deven McGraw – Center for Democracy & Technology – Director

So, my colleague Dixie Baker is going to manage this particular panel. Again, can I ask for all extraneous conversations to please try to take it outside. Thank you.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

All right, our final panel today is on trusted identity solutions in the federal government. We have three people listed for this, but only two of them actually will participate today. The first participant is Troy Trenkle, who is the Chief Information Officer at the Centers for Medicare and Medicaid Services. We welcome you, thank you Tony. The second is an individual who's on the phone, Cynthia Bias. She is with the new Integrated Electronic Health Care Record project which, for those of you who may not be familiar with the iEHR, is the shared electronic health record between the Department of Defense and the

Department of Veterans Affairs. And Cynthia is working in identity and access management at the integrated program management office for the iEHR. So, with that, I will turn it over to Tony.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Thank you, Dixie. I'll spend a couple of minutes, I guess I have seven minutes to talk about the history of CMS and identity management. Go ahead and get this off here, be better. So, I'll try to do it in seven minutes but if I take a little longer, sorry about that. So let me move to the next slide, which I can't read from here so…I feel like I'm at the end of a football field. But anyhow, I think you are familiar with this. We have a number of drivers that we face for healthcare credentialing and validation. This has been something that has been going on for a number of years, and I didn't put together these slides, so if I don't talk directly to them, let me just kind of cut to the chase with it, we have a number of provider authentication systems already at CMS.

One of our drivers has been with the Affordable Care Act, is looking across our enterprise and seeing exactly how we can support a multitude of projects that traditionally CMS has done in a programmatic, stovepipe manner. We have the decentralized IT shop, although I'm the CIO and Director of the office of information systems, we have a number of other IT shops around the agency. We also do not have, like places like SSA and other similar government agencies, we don't have a centralized authentication policy shop that looks across the enterprise in terms of how to bring together from a policy and a technology standpoint some of the identity management authentication authorization solutions. So the challenges we face are twofold; one is dealing with a fragmented infrastructure, both policy, business and technology. And then also dealing with a need on the Affordable Care Act, to improve how we do identity management to support a number of different models of improving health care; whether it be working with accountable care organizations, the insurance exchanges or any one of a number of other areas where identity management not only from the providers side, though I think my remarks they're limited provider side, but also from a beneficiary or, I don't know if the right word is citizen consumer or what, as each of them has different definitional attributes. But, from a number of angles, we've had to look at this and the drivers are both internal and external, I think that's the point I am trying to make here.

So, we're not in this alone. There are a number of other organizations who deal with the same providers. We have a database of almost 4 million providers in our NPPES system, people have gotten NPIs. We have almost a million providers in our Medicare provider system, which is called PECOS. We also have providers who are in the Medicaid space, who we get information. We have a number of other areas where we interact with providers, both inside the Medicare fee for service but also the Medicare advantage and so, we face a number of things internally but then externally, as I said, a number of these organizations and providers actually deal with the Social Security Administration, the VA, Department of Defense, the Drug Enforcement Administration in terms of the e-Prescribing of controlled substances, health plans, a number of other areas we have the exact same individual who is dealing with, when I say individual, I'm not just talking about the providers themselves, but also the providers staffs, who as you all know, do a lot of the data exchange work with us and other entities. Of course, with the outgrowth of affordable care, we have new organizations popping up as well. So, the traditional CMS way of doing it in a programmatic stovepipe method is no longer not only feasible from an expense point of view, but also will not work in the New World of health reform.

Next slide, there we go. So, in the last year one of the things we focused on was developing a number of enterprise shared services in CMS and two of them that are really relevant here, one is enterprise identity management and the other is a CMS portal and they kind of work hand in glove. So what we're trying to do is create an enterprise portal within CMS that will allow different entities, whether they be providers, beneficiaries, whatever, to come in and get a…go through a series of steps where they can get credentialed or actually, use an existing credential and then work through the access and authorization process so they can go to multiple types of applications. The idea here is, this not only helps us from a privacy and security standpoint but also from a user ability standpoint, this provides a lot of improvements. So, we were awarded a contract in January on remote ID proofing, but our major enterprise identity management project was actually awarded several weeks ago and the prime on that is QSSI and they're using a number of subcontractors on that. A basically the idea is over the next six months working in coordination with the insurance exchange work, working in coordination with the accountable care organizations, some of the other affordable care act work, is to begin to stand up this enterprise identity management solution and portal.

Now, it won't be all perfect on day one, but over time we want to consolidate what we have and continue to grow that as we go on. But, I think the idea here is this is not something that's going to happen over the next couple of months, but it's going to happen over several years. Several of the things that we're very much focused on is being very supportive and coordinated with the work that ONC is doing, with the work that Jeremy Grant and the NSTIC is doing. We want to use FICAM certified credential providers, we worked with ONC on some of the language and the statement of work, as well as Jeremy. We've been very involved in the work groups that Jeremy has stood up under the NSTIC work, the FCX federal cloud credentialing exchange, or whatever it is; I don't have the acronym in front of me. But, the point of the matter…Lisa knows, and you've all heard Jeremy earlier today, that the point is we're not doing this in a vacuum. We are doing it together in partnership, not only within the government, but certainly I'm going to work with industry and others on this. We've come a long way in the past year and we're just about at the point over the next several months, we're going to stand this up and this is basically the timeline where we're at today and where we are trying to go in the next number of months.

Of course we have a number of looming efforts that are going on, both in the accountable care world and also in the insurance exchange area that are driving us towards moving ahead, as well as program integrity, that's another big driver in this area. One of the things under the Affordable Care Act and as well under this administration, is there's been a real push towards improving program integrity, so identity management and improving our PECOS system has been something that's been at the forefront. Another area that's been in the forefront is tying in the Medicare and Medicaid program much closer. Of course Farzad, I know you're familiar with the work we've been doing with HITECH, but also do eligible, looking from the Medicaid side, how they can improve the quality and quantity of data we get from the states. And so all of these are drivers that are moving us forward, and they're all going to be tied into this identity management work that we're going to be doing from an enterprise perspective. So, I think I've gotten close or slightly exceeded my seven minutes, so I'll turn it back over to, I guess Dixie, right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes. Thank you very much Tony. Okay, and I understand that Cynthia is on the line. Cynthia?

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

Yes, I am, thank you.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Thank you.

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

Good afternoon everyone. I apologize for not being able to be there with you in person, but I do thank you for the opportunity and the invitation to present today. I would try to move quickly due to time constraints and the presentation. I did want to take a moment though, however, to introduce one of my cohorts who was there in person with you, Miss Janine Groth, from DOD and one of my partners for iEHR. On slide number two, I wanted to quickly just provide an overview of what I'll cover today and will give an interview…excuse me, an overview of the electronic health record. What we're going to be looking at for initial operating capability, the plan that we're going to use for the authentication and authorization for our providers that are going to be accessing the systems, and go over some of the challenges in the identity and access management areas that we will experience in iEHR.

Next slide. One of the things that is very prevalent within iEHR is this is a massive undertaking to join all of the healthcare information from the Department of Defense and the Department of Veterans Affairs. We have hundreds of medical centers located throughout the country that have records contained within their systems and we are looking at making one very large repository and system throughout the country for both agencies. So, it is a very daunting undertaking. We do want to better serve our customer population, which usually initiates with the Department of Defense and then they transition into the VA as they become a veteran and separate from active duty service. We want to be able to increase the level of visibility into the medical record for our physicians, so there are some cost savings associated with not having to repeat medical tests or undergo various investigations that the employee…excuse me, the veteran would have to undergo to be awarded benefits and things of that nature.

Next slide. Some of the things that we are looking at for our initial operating capability within iEHR are putting into place the foundational services, and this is where the identity and access management area falls. We are required along with things such as SOA, the portal, the user interface, etcetera, to be able to present information on our joint system. I did want to highlight within the iEHR scope, we are looking at the identities of the providers or our healthcare providers I should say, and other computer users differently than we are looking at the identity for our patients. So I did want to point that out that sometimes that is lost in the identity and access management discussions, but they are actually handled very differently for purposes of i EHR. We have scoped the initial capability to the outpatient care setting. So the intended goal for iEHR would be to have a presentation layer of some type that the physicians will access during their point of care interaction with the patient. So this could include providers, nurses, physician assistants, anyone that would have the direct interaction with the patient.

Additionally we were looking at adding capabilities from the laboratory, pharmacy and immunization packages. So, as we were looking at scoping the entire effort, we're not undertaking all of the various is capabilities in a medical record in this joint venue, nor all of the users in this venue. So, we are trying to scope it in such a way we can actually succeed.

I did want to highlight this does include both the Department of Defense and VA computer users that are going to be providing care. We also have limited the locations and we are targeting the initial release for 2014. There was a lot of work going on within the iEHR space to determine the final or full operating

capability, so that still continues to unfold as we work towards the project. Next slide. So this is the slide that really interests this group I would imagine. One of the areas within access control that I personally am proud of is the fact we are not planning to issue iEHR credentials. We are planning to reuse credentials that exist. So, for our initial operating capability, we do plan to use the DOD's common access card and the VA's personal identification or PIV card, that are both HSPD-12, level 4 compliant cards. Because of the scope of iEHR and the fact we are limiting the user base, these will be the only credentials accepted for our initial operating capability. We may come across a few exceptions that are specific to VA or DOD, but these are the predominant credentials that will be accepted. As we move forward with iEHR, there will be self-service capabilities for the veterans or family members or delegates, etcetera, to be able to access information related to the veterans' health record. These capabilities have not yet been fully fleshed out for iEHR, and what we'd like to see in the future, but there are definite plans going on trying to determine what those are in the future.

As we move forward with additional increments of the iEHR releases, because this will be a many year effort, trying to enable all of the capabilities throughout the medical record, we are looking to add additional credentials that iEHR would accept. As each of the business use cases are developed and further defined, the iEHR team will determine which credentials we choose to accept. Some of the examples that are currently viable, the DOD/DF logon credentials is a self-service credential that's currently issued by DOD and is currently accepted for a variety of purposes within the VA, including the e-Benefits portal. So we do intend for that credential to become one of the self-service credentials accepted. There are opportunities to add additional credentials again as the use cases present themselves. If we find a large population of users who have a particular type of credential that has been deemed

acceptable before iEHR, we would consider using that credential. We already have had some discussion related to using additional agencies PIV cards, also HSPD-12 complaint cards. And, at the present time I would assume that those credentials would have to be level 4, but I have heard some discussion throughout the day relating to some cards being level 3. But, I would assume were going to mandate level 4 for certain types of access.

Additionally we have considered the PIV-I cards. This is an area that I think continues to grow in this sector and will become more and more valuable as that continues. We do have as contractor support, many large companies that are interested in looking in the PIV-I issuance for their corporate users, and that is of interest to iEHR and the agencies as a whole. We do currently accept some FICAM credentials in the VA space and we are looking to expand this into the iEHR space, as the use cases require. And additionally, if there other credentials that become available, I know inside of the VA itself they have been working with CMS to look at accepting their credentials, and I would hope that work would be taken advantage of, as we move forward with iEHR in the future.

Okay, next slide. I just thought I would list a couple of challenges that we have within iEHR, and one of them I think has been discussed throughout the day, is the mechanism to associate the credentials from various providers to an iEHR specific user, and be able to marry that user up with their authorizations that we have designated for iEHR specifically. We are looking at using role-based, rule-based and attribute-based authorization techniques, but we do have to be able to ensure we are associating these authorizations with the correct individual. One of the additional challenges in that space is the fact we will have individuals that have multiple credentials. So for example, you may have an individual that is active duty military reserves, they're an active VA employee and they also have one or multiple self-service credentials. So, we will have to mirror…match all of those individuals, their credentials and authorizations so that way we can support separation of duties and things of that nature and be aware of when a user is coming in in the self-service capacity or a capacity to do their job.

And the last one we wanted to list was the ability for all of our partners to obtain a credential that we can use by the decision of not issuing iEHR specific credentials, we did open up ourselves to a large risk in that we do need to have credentials available for all of the business community that we wish to interoperate with. This could include private sector physicians that our patients are referred out to. They could be private sector laboratories or pharmacies that are tests or prescriptions, things of that nature are designated to for fulfillment. So, we do have a lot of partners that we will be looking at integrating as we move forward with iEHR. Again, those particular users are not in the iEHR initial operating capability, so we don't have a formal plan for those at this time, but it is something I wanted to make the group aware and share that as a potential issue. And that is the conclusion of the presentation, so I will turn it back to Dixie.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Thank you very much, Cynthia. Okay, it's time for our discussion and as the chair's prerogative, I am going to ask Tony a question. You mentioned, and this is something we've had many discussions about, you said that CMS will use the FICAM certified credential providers. Does that also mean that you will also require that private hospitals and practices use credentials that are issued by a FICAM certified credential providers.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Yeah, that's part of it. Dixie, let me just mention a couple things. One is we don't want to become the credential provider for the world. We want to become a relying party so, we definitely don't want to be in the credential business ourselves. So to us it makes sense to use the FICAM certified providers. Now, how that will work with the hospitals and other providers is something that we're going to have to work out some of the policy issues around that. So at this point, I can't say that we're going to make that a requirement, but that's something we have to look at. Obviously if we're going to do business that way, we're going to need to have them utilize a credential that has some type of certification, whether it's…and our goal right now is to use the ones that are FICAM certified, to be in coordination with the rest of the federal government. But obviously that's something we have to continue to look at as the policy continues to evolve and we'll certainly be looking at that from a regulatory standpoint and getting comments back from industry as we move that direction.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay, thank you. John, oh Walter?

W

We thought you were jumping way early into the queue.

John Houston – University of Pittsburgh Medical Center

No, I don't think I can.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Walter.

Walter Suarez, MD, MPH – Kaiser Permanente

Thank you, this is Walter. Just a quick follow-up on that, what's the timing for that…in terms of adopting requirements for individual providers, let's not talk about organizational providers, but individual providers to use …to be certified through a FICAM kind of system, what's the timing for that?

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Well the timing to get the system set up will be later this year. We are going to be moving towards it with more complete implementation next year. In terms of the timing as far as requirements, as I say, that's something we're still going to have to work through with our policy folks. It won't be something that will be applied to every CMS business line initially. It'll be something where we start in certain business lines and then kind of work through some of the issues both technically, operational and policy-wise and then move towards a more coordinated approach. But the goal is to make it something we do enterprise wide beginning next year.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Are these credentials…that's a great question Walter. Are the…when you talk about credentials, are you talking about individual person level credentials or are you talking about organizational credentials or both?

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Initially it will be person level credentials.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

I just want to say, in Tony's usual understated way, this is a big deal. For CMS not to say we're not going to be the only using credentials that we contract for, but instead, we're going to accept a variety of different FICAM certified credentials and we see ourselves as a relying party and kind of a member of the ecosystem it's a…this is a big deal. And I want to thank Tony and his team for really the terrific

collaboration across the federal agencies and with NSTIC on this.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Yeah, thanks Farzad. Yeah, and I think that's a critical point. We don't want to be behind where the federal effort is, we don't want to be ahead of it, we want to work very closely with Jeremy, with Farzad and others who are working to develop the identity ecosystem. And we want to make sure, as the key player in this, that CMS is in lock sync with that, both from a department HHS standpoint, federal government and a healthcare industry standpoint. We're not out to create the universe, we're out to help others, working with others to create the universe.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Thank you. David? Oh, I didn't even see that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I was going to make sure you saw it. David McCallie. Tony, you may have answered this and I just missed it, but, you referred to the remote identity proofing. What standard will be used for…or what approach or requirements for the remote proofing? Will it follow the NIST 800-63-1 that we've been discussing all morning?

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Yes, exactly. We had set that up as something we initially felt we might need from a program integrity standpoint, but as we move along, we may…we probably will use that less and less, but yes, we'll be in coordination with the NIST standards. Most of our providers and actually most of our applications require level 3 authentication and that's kind of how we're building out infrastructure to support that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And then leveraging on that, assuming for those who do use formal level 3 and pass muster. For Cynthia, a question. You listed the identity providers you would accept and the CMS processes to be determined in the future, as I recall from your slide, and my question is what's the reason that if they have level 3 based process that's done by a certified FICAM organization, that they wouldn't be accepted immediately as valid credentials in the iEHR system? And what I'm really looking for is what are the barriers, not an explanation of why you made that decision.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Are you talking about…well, the iEHR, that's Cynthia, are you asking that question to Cynthia?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yes, yes, it's a question for her and I'm using you as an example…

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Okay, I'm sorry.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

…because CMS was…the FICAM approved providers was down in her futures and the question is, what's the barrier for accepting those credentials if they meet the FICAM process and the NIST level 3 assurance. Why is that something to be determined in the future. It's really to the interoperability of trust question here, I'm again trying to figure out what are the real world reasons why that isn't a simple decision, for Cynthia.

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

The comment that I made isn't really due to trust, it would be due to user cross-population, if that's a good term to use. So, as we are looking at implementation timelines, cost to integrate with additional service providers, things of that nature, we would want to select the providers that have a large population of the users that we anticipate. So, and it also speaks to a governance perspective. We do plan to have a list of credentials that iEHR has elected to accept and that would be of formal process, a business process, that we would go through inside of iEHR to have those credentials approved for use by iEHR, not that they are meeting…or that they would or would not meet the FICAM standards, things of that nature, that would be assumed if they're a FICAM approved credential. So, it's not necessarily an interoperability issue, it would be a time to implement, things of that nature. It would be desirable to offer as many

credentials as possible, but that again would have to be a business decision that we in IT would support. So, it's not necessarily an interoperability, it's more of governance type issue, if that makes sense.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

This is David again. And that's a great answer, thanks for that clarification. But that is exactly what my

question is, why is that a business issue that requires a governance decision? In other words, if the goal of NSTIC is a universal identity, a universal trust around what it means to possess a certain credential, then why are there barriers as to accepting those credentials? I know in the real world these are very commonly there, I'm just trying to understand what they are, what those barriers are.

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

So, from an implementation perspective, we would want to know first off the credential that we're choosing to accept and the identity provider, the business rules that they used to issue those credentials. So if they're FICAM approved or some standard that's recognized, then we have that to go forward with and that would remove some of the interoperability questions. The governance is just a due diligence to say these are the credentials that are being accepted, so that way we can technically implement them, set up any of the IAAs or any type of legal agreements that need to be put into place to utilize the credentials and that way everything we do does have a legal perspective to it, based on the fact we are utilizing that credential appropriately. I mean, there would be requirements on the iEHR side as well, that we are only doing with the credential what is allowed for use. So it's again, not a barrier, it's just a process that would need to be adhered to as we move forward, because we're not going to open up a healthcare application to just any credential out there without doing a technical integration and a governance process approval. Again, just a process to say that yes, we have chosen to accept that credential, we'd have to update our website to show that we're accepting that credential so that the users would be aware. Depending on the type of users, there could be an educational aspect to it that we may need to be sending out information saying, hey did you know we're going to start accepting this credential, things like that. So, it's not just about the interoperability capability of the credential itself.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

David, can I offer an example? I mentioned to my folks this morning, they didn't have an answer for it. The way we keep up our PECOS, or Medicare provider file, one of the things we do is we get the death master file from some SSA, which tells us which providers have died. One of the things I asked my folks is, suppose we get a credential from an organization that's certified by FICAM, it has Doc Jones. We find that when we go against our PECOS file, that Doc Jones has died, according to the SSA death master file, but yet it's still being maintained as a live credential, so someone, maybe Doc Jones' spouse or someone else may be using Doc Jones' credential. So what's the process then for revoking Doc Jones' credential if we find, based on our records, that we have a have a discrepancy between the Doc Jones in our records and the Doc Jones credential that's come in to us. And maybe Jeremy's worked that out, but my folks did not have the answer to that, but that's just one example. You may have a great credential service provider system set up, but you have certain governance things we need to kind of work through internally, within our own agencies, because of these types of potential issues that may come up.

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

This is Cindy. Additionally, if I would add to that, there is the authorizations that need to be put it into place for that credential holder. So within iEHR, we do have to have a way to recognize that this person, coming in with this authorized credential, should be allowed these specific permissions within the system. So, we also have to have a way that we are implementing to ensure we can associate that credential with the appropriate permissions within the iEHR system. So that does speak to some level of technical integration work that does have to be implemented. So again, just speaking to priorities, timelines, dollars and things of that nature, we would prioritize certain credentials in a certain order based on how many users we think we would estimate would hold that particular credential and would be of the most value to iEHR. We would start there first and expand after that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So, this is David again. Just in response to that, again, that's very clear. I think there's obviously a distinction between the trustworthiness of the credential and whether or not that person has any right to access your system, and you're going to manage the latter regardless of the trustworthiness of the credential. So, my question was, what are the barriers in trusting a FICAM, NIST level 3 compliant certified credential, other than interfacing costs?

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

Um, there's really not one, as long as that is the desire for the iEHR board.

Janine Groth – Department of Defense

Cindy, let me take a stab at this. So, the DOD and VAs intention is to fully support the FICAM credentials, correct Cindy?

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

Correct.

Janine Groth – Department of Defense

Okay. So then, in terms of the timing, the timing is more driven by business decisions around iEHR scoping than it is about implementing FICAM credentials specifically. So, the IOC phase that Cindy spoke to, is a very narrow scope of what we're just trying to get up that's joined for DOD and VA, for the direct providers that are employees of DOD and VA. As we go to subsequent phases, when we bring more functionality into iEHR, then it becomes more appropriate to start talking about the FICAM credentials in the context of reaching out to the commercial providers and the network. So that's really what's driving the timing versus any concern about the trustworthiness.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So, I think you said it as you were on your way up to the microphone, let me make sure I heard it correctly, the trustworthiness of the credential is not at issue.

Janine Groth – Department of Defense

Correct.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

It's really the nuts and bolts of hooking all the pieces together.

Janine Groth – Department of Defense

Correct.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And that's really what I was aiming for is that if we ever hope to achieve anything remotely approaching the NSTIC vision of universality with trust, the trust has to be universal, at the appropriate level of assurance, otherwise we're just wasting a lot of time because if you have to go through the n-squared

arrangements to reestablish trust every time you bring in a new credential source, we haven't gained anything.

Janine Groth – Department of Defense

And Cindy, I just wanted to make sure you concur with that.

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

Correct. That is what I was saying, that there really isn't an issue related to the trustworthiness of the credential, that's why I spoke to the training and implementation and updating portals, things of that nature. So, it is really an implementation effort, looking at the best use of the iEHR dollars and integrating with the credentials that provide the most value up front. As I shared in the presentation, we are using credentials outside iEHR from day one. So these are DOD issued, VA issued credentials that we are using for this joint system iEHR system. So from day one, we are in a federated trust model, so that is the go forward strategy, too continue that venue. And as I listed, one of the challenges in our presentation is the fact we want to ensure that all of the partners that we do want to have accessing the iEHR system have availability to obtain one of the trusted credentials that we can use going forward.

Janine Groth – Department of Defense

And I think Cindy brings up a good point that what we are doing with using the CAC and the VA PIV is a really good example of HSPD-12 interoperability. And then the support for the single sign-on based on that.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

Yeah, I think that's a good point. We are also, of course, abiding by HSPD-12 and we credential our employees, a number of contractors, but in addition to that, we have a number of others outside our, what we call our inner circle, that also have direct access to our systems, someone who may be providers and in that case we may decide to issue like a PIV-I card or some other type of credential, rather than…well, it just has to be kind of worked in with the whole FICAM infrastructure as well, because different types of relationships require different types of not just trust, but also business decisions and policies because of the way people work with us.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I have a question about direct, the direct transport protocol where the identity is at the organizational level…for both of you actually…is at the organizational level and not at the individual level. Is that going to be an issue for you, will you still be able to accept connections that are authenticated at the organizational level rather than the individual level?

Cynthia Bias – U.S. Department of Defense/U.S. Department of Veterans Affairs Integrated Program – iEHR Identity Management and Access Management Project Manager

I'm not sure I follow the question, so, we do currently support SAML for…well in the VA space and the DOD space as well, not yet in the iEHR space, but we do support SAML coming in from federated partners, etcetera, is that what you mean.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

No, it has nothing to do with SAML. It's the connections are either…currently either over the NwHIN exchange protocol or stage 2 meaningful use is likely to require the direct…using the direct protocol which is really e-mail based, and the certificates that are used for authenticating those connections are specified to be at the organizational level, not at the individual level. So I'm asking whether that's going to have to be revisited once you start receiving those kinds of connections.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

We've worked with direct on a pilot basis for several years now and that's one of the things we're going to have to see how we can integrate that into this identity management solution, I'm sure. Several of my staff have already looked in to that, but I don't have the answer for you today.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Thank you. Are there other issues? Walter?

Walter Suarez, MD, MPH – Kaiser Permanente

Yes. this is Walter. First of all, this has been a very exciting day, thank you for putting it together and thanks for all the testimony. It has been an amazing moment I think listening to particularly this panel where we hear, and we already know that VA is requiring a much higher level of assurance that just class 1 and 2. We're hearing about the implementation of a level 3 plus level of assurance by the VA and now we're hearing, certainly CMS is going to move into requiring that type of a level of assurance from individual providers. And so, in many respects the issue…or the question now becomes not so much whether we will see a movement towards that type of a level of assurance, but more when are we going to see it and it sounds like it's very quickly coming up. It's going to be 2014 or around that time when we're going to see that and the example of interoperability that David was asking perhaps, is better illustrated perhaps with; I am a Medicare provider, but I'm also a provider that delivers care to the VA and DOD. Am I going to have just a single certificate, a FICAM based certificate, that will work for both Medicare and for the VA and for anybody else at the end of the day, because I am going to be delivering and prescribing drugs at the VA, requires me to have the type of levels of assurance. So, we're reaching maybe what people would say is the critical mass of pushing the industry to the next stage. And I just wanted to confirm that, I mean it might sound like an odious statement, but that this is the case, that in reality what we are seeing is a movement towards adopting a level 3 at least level of assurance or Class 3 level of assurance, FICAM based, that is interoperable across for example federal agencies and beyond that across HIE systems like the ones that we heard earlier.

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

I think a number of us have been working in this space for years and where it's collapsed before is at the central governance management level, and the question now is, I think, the momentum that Jeremy and his team have put together is very impressive. That if we can continue that and get to the point where this becomes like the credit card or whatever industry you want to utilize…use as an example, where we come up with an infrastructure that is supported financially, it comes up with the right solution for that from risk management, everyone is comfortable with where we're at from an operational and governance perspective, I think we're going to get there Walter. I think where it's collapsed before is initiatives have started, have not continued momentum. Agencies on their own, we all have tight deadlines to meet. We have legislative and other mandates we can't just sit down and wait for the grand solution to come through and stop all the work we are doing. So, I think we are at a critical point now and I think we've made a lot of progress in the last year with the work that's been done, but it is a good question. Are we now at the point where we can move beyond just an idea and a dream into something that's an operational reality that scales to the level we need to do to make this successful? And that's going to take some push from everybody.

Walter Suarez, MD, MPH – Kaiser Permanente

Thank you.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Are there other questions, other cards I may not see? Yeah, John?

John Houston – University of Pittsburgh Medical Center

I'm following up on Walter. What do you think a rational time horizon is, in terms of putting this in place? Is it one year, two years, five years…

Tony Trenkle – Centers for Medicare and Medicaid Services – Chief Information Officer and Director, Office of Information Services

I don't think it's a rational timeline; it's something that's not put into place, but something sustainable and that grows over time. I mean, if you put something into place tomorrow and it can collapse a year from there, it's something that not only has to be put into place, but something that is operating around an agreement from whether you want to call people members of this or whatever that we work together to make it continue to operate. If that doesn't happen, then it doesn't matter whether it gets put in place one year or five years from now, it's not going to be sustainable.

John Houston – University of Pittsburgh Medical Center

Good point.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay, well thank you. I think we're ready to move for a general discussion.

Deven McGraw – Center for Democracy & Technology – Director

Yes. So, I thank you very much Tony, Cindy and Janine. Thank you very much for taking the time, we very much appreciate it. So, we've got a little bit of time on the agenda in order to prompt a little bit of…it's labeled a discussion in the agenda, but I would call it more of a kind of sharing of thoughts and impressions from the hearing that can help inform some future deliberations. The Tiger Team has two calls scheduled to discuss what we've heard today, to come up with potential policy recommendations for

the policy committee to consider at its August meeting, which is actually on August 1st. And so again, we're not trying to come to consensus among our two groups necessarily. We're each still going to report to our respective committees, but I do think it's helpful having just heard a lot of really good testimony to take a few minutes while we can to just sort of share our own thoughts about this and maybe engage in a little bit of discussion that, quite frankly selfishly from my point of view, will really help…could help inform how the Tiger Team goes about forming some of its policy recommendations on this issue.

John Houston – University of Pittsburgh Medical Center

What's the Tiger Teams charge in terms of what are the tone of recommendations supposed to be?

Deven McGraw – Center for Democracy & Technology – Director

Well, so in my view, we haven't been asked a specific set of questions other than to say that we teed up some recommendations already to the policy committee that now one could argue are a little outdated, or certainly don't take into account recent developments with respect to both NSTIC as well as the new release of NIST 800-63-1. But there have been some new developments, so it gives a chance to reassess that. Certainly during our discussions on the RFI for NwHIN, that period of time has closed, but a similar set of issues was raised. We left open a number of issues, even with respect to the recommendations that we made. And so, I think in light of recent developments I think our charge is really to think about whether the recommendations that we initially made about more than just username and password for remote access, what does that mean in light of…again, in light of NSTIC and the NIST factors, which have been revised and that initially we weren't sort of comfortable landing on something. And a desire…an interest expressed by Dr. Mostashari that if there's a way to get to a higher trusted level 3 in a way that would work for the industry, that we should consider that and think about how we would do

that. Is that a decent articulation? Do you want to add to that at all, Farzad?

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

Yeah, just to maybe rephrase, one thing…

Deven McGraw – Center for Democracy & Technology – Director

Oh, to contradict, too.

Farzad Mostashari – U.S. Dept. of Health and Human Services – Office of the National Coordinator for Health Information Technology

No, no, not at all. One thing that I think the Policy Committee and Standards Committee to some extent would benefit from hearing, would be a summary of what we learned today. So what has changed, what are some trends and developments that might have relevance? That's one. In light of that, whether there

is a change in our assessment of the feasibility of widespread level 3 credentials for healthcare providers. And then, I think the policy discussion to come would be then what would be the context and the use cases in which level 3 identity proofing and identity assurance would be appropriate? Is it just remote EHR access? Is limited to exchange and whether there are implications of that for our next cycle of rulemaking? Those would be the kind of teeing up the discussion for the Policy and the Standards Committees to consider. I think another factor here, is the extent to which we heard from DEA as a driver for two factor authentication, we heard from CMS, saying they are policy drivers for helping create this ecosystem. And we heard from the iEHR with DOD and VA potentially being drivers for this. And I think the question for us is whether there is an obligation or opportunity for us in the health IT space to also be a driver for this new ecosystem of identity assurance for healthcare providers at level 3.

Deven McGraw – Center for Democracy & Technology – Director

Okay. So on that note, would anyone like to start? Oh David, I can always count on you. But this is really actually very much appreciated. Go for it!

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I could talk about anything I want and you'd appreciate it. So, I haven't synthesized all this yet it in my head, but I heard a couple of things that I think we could pursue, one of which is this notion of using an organization as the identity proofing entity, as opposed to requiring every individual to get proofed externally, is absolutely a keeper idea. It's being well deployed in the field today by numerous organizations, but the federal FICAM cross-Ts-dot-Is details of what it takes to actually pass muster for doing that is still unclear. So, I got the sense from one of the panelists, and I'm going to forget their name, that the FICAM process would be happy to accommodate a specific set of rules on how that ought to work if someone would ask them to. And it was sort of like, we could make that work, remote proofing outsourced to the organization after the organization has been vetted appropriately and make that a part of a FICAM certification that would pass muster with others level 3 certificates, just ask us to. So, if I heard that right, we should ask them to, and get that process down. Dixie?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah, just want to make sure I'm capturing…NIST 800-63 says what is required for level 3 identity proofing, but what you're saying is a need for a process and requirements for using a third-party to do what's in there for level three?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Right, for the organization itself, not a generic third-party as in, you know, an open RP but the actual organization taking on that responsibility and doing it in a way that could meet FICAM trust provider certification. So, if you go to the website today, it only talks about certifying of individuals. But I've heard from them that they don't have a problem with doing it through the organization, it just needs to be written down. So, if that's the case, then to Farzad's question, I'd say we are ready to move to widespread level 3, once you can nail that down, because organizations are already doing equivalent to level 3 proofing of their internal users because they're medical organizations, they have to be incredibly careful about who the users are. The gap is not that we don't know who the doctors are that are on the systems, the gap is that we don't have a standard way for that to be trusted by everybody else and the federal government. And so, we have robust credentialing in place in all the hospitals and doctor's offices already, through the states and whatever. We just don't have a formal way to put it into a regulation that says, if you get your credential through this FICAM certified process, we'll trust it.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Level 3 does allow remote ID proofing.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Right, but it's not on the FICAM webpage…I mean the approved providers that are out there, the non-federal providers of those credentials, as I understand it, does not include that use case, going through an organization.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Where that organization is a third-party; it's is like Kaiser, it's like Kaiser going out to a third-party.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

No, even Kaiser. In other words, you can't get a credential through Kaiser, through Kaiser's internal certification process, their provider credentialing process, you can't get a FICAM trusted identity at this point.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Just to clarify, the one vendor, Verizon, who that is certified for NIST LOA…for FICAM LOA 3, NIST LOA 3, does use remote identity proofing. There's another one that will be there shortly, probably in the next month, they'll get a certification, also uses remote identity proofing. So, that is supported today, but it's only those specific credential providers who've gone through the certification process. An organization like Kaiser wanted to be able to issue those credential themselves, the way would to do it would either be to contract with one of the providers who already has that certified solution or get certified themselves with something comparable.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So to me that seems to be the barrier, because becoming certified yourself is expensive, cumbersome and it is unlikely for anybody but the very largest healthcare organizations to even dream about doing that. And yet, we heard examples of well-functioning HIE's, the Washington State 25 or more RPs and 50,000 identities managed and healthcare data being shared, apparently safely and securely, done with local proofing, proofing by the organizations themselves, and that proofing could meet level 3 standards, if we wanted it to.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

That could be in-person identity proofing at that point, which would be considered stronger than remote identity proofing.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

That's level 4.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

But, my point is that provider organizations already need in person proofing in order to let a doctor practice inside their boundaries, and the doctors staff; I mean, they have gone way beyond even level 4 probably. But we don't have a way to connect that real-world certainty about who these users are to a FICAM process, without the expense of bringing a third party organization in.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy

So one of the things that Deb Gallagher talked about just briefly today, and I might be able to expand on a little bit in a further discussion is while NIST 800-63 does not separate levels of assurance for the identity proofing side and the credential side, GSA has been looking at that because there are some solution providers that might say, hey, if I can already show that I've done valid in-person proofing, can I then bind that to a credential? There's an effort underway our office has actually co-sponsored setting up a technical committee within OASIS, looking at the concept of trust elevation, which essentially looks at, if I have a credential at let's say level 1 for starters, I don't know anything about you and you have a username and password, what steps can I then bring you through to elevate that to the right level credential for a particular application? The idea being that somebody might come say as a veteran to the VA, who's unknown, but they can put them through some processes that could elevate them both through identity proofing as well as the issuance of a stronger, multifactor credential that could be bound to…5:33:05 . That technical committee's still finishing up its work, but some of that is within the roadmap of what their office and our office is looking at, as a way to add more flexibility to what are, I think arguably, some rigid certification processes today. What's that, oh, sorry, this is Jeremy Grant from the NSTIC program office, just decided to sit down at the table and talk.

Deven McGraw – Center for Democracy & Technology – Director

Thanks, Jeremy that actually was really helpful. Were there some others, David, before we move on? I mean, not that you won't have lots of other opportunities to share, but…

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well, I mean, to me, that's the one that we keep stepping are toe on over and over again, so that's the high priority one. The other observation is simply as was quoted at the first panel, the barriers aren't technology, the barriers are getting people to trust each other in ways that have nothing to do with cryptography, which has to do with the fact that as they decide to do business with each other, in the current models, they're in pair by pair, n-squared relationships, and that's not going to scale. So either we give…we either have to get everyone to agree to trust, based on cryptographic and procedural standards, like FICAM standards or, we just don't try to scale it and we don't go for NSTIC, we just do community by community, which is sort of what we've got today, and it doesn't work very well. Certainly for some things it works okay, some things like CMS it doesn't work very well at all, because CMS has to talk to everybody.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I don't quite understand and I hope you can explain this to me. Within the…to get an HSPD-12 certificate, like at the company I work with…work for SAIC. SAIC buys a whole block of these credentials and then SAIC then individually requires face-to-face authentication in order to give you this card that has a smart card, that has the individual certificate on it, which is exactly what David is calling for, only in the DOD space, right. But why is that not…well, its federal space, yeah, you're right, it's federal space. Why is that same process not…why can't it be that same buy a block of certificates at Kaiser, and do the same thing for health credentials? I don't understand…

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

The difference is, SAIC, you work for SAIC?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

So your firm, because you're a bigger aerospace defense contractor, has most likely gone out of its way to become certified as a PIV-I issuer, with a certificate authority like CertiPath, that is…we didn't talk so much about PIV-I today…

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yes, they buy them from…

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

…LOA 3 is the floor, but when you start to get to level of assurance 4, which are these PIV cards and PIV-I cards that are out there, frankly when we're talking about an environment like the VA or the DOD,

where the medical facilities are all owned by the government and the doctors are government employees, it's great that they already have a level 4 credential, because 4 is better than 3 in the whole scheme of things, at least when it comes to security. So if your firm…there are basically two ways as a government contractor that you can get a PIV card. One is if you were working on site for government clients, so for example, the DOD or my agency at Commerce, if you're working for us, we'll give contractors PIV cards that have a green stripe on them, and some changes in the information on the chip, shows they're contractors. But a lot of the big firms have also signed up as PIV-I, in part because they're building

information sharing frameworks between the big firms that are working with each other. A classic example is the Joint Strike Project, which is being built by how many big firms and so the aerospace defense companies have set up an organization, TSCP, Transglobal Secure Collaboration Program, that allows them to use PIV strength credentials to share information say between SAIC and Lockheed on a component of an airplane. So, you're firm's offering today I think has made the investment to actually become an issuer, and maybe they did it on their own, maybe they did it by joining one of these consortia, we haven't seen that in the health community yet, but there are business cases certainly there as well as universities that form trust frameworks where they trust each other…

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But the process that David's asking for must be defined somewhere, right?

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Yes, it is. in fact, it's part of the FICAM roadmap that Deb Gallagher's team at GSA puts out. So, when we talk about FICAM, we shouldn't overlook PIV-I, there's been a lot of talk today about level 3…

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

But she's not just talking about PIV-I, she's talking about the…and this I believe this is set out, at least as at the federal bridge. I haven't looked at the FICAM documents, so I'm just talking about PKI here, so it's a more limited universe, but there is a process there where somebody can become

a certificate authority.

Jeremy Grant – National Institute of Standards and Technology – Senior Executive Advisor, National Strategy for Identity Management

Correct.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

And they issue…

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

…you know, you're doing the identity…

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

They do the RA and the CA functionality, and they get that…they…in the healthcare sector they've been talking about these HISPs, the health information service providers potentially as serving in that function

because they may be large enough to step into that. They may…since you were looking for a potential healthcare example of doing it. So, it's not unheard of, it hasn't been discussed. You've heard this, right David, a little bit.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yes, absolutely. My thought was that we want to make that scale better without requiring the complexity…as it is now, to become a HISP, if you go through what direct trust and others are proposing based on the governance RFI, read between the lines and see where the trains headed, it's a big, complicated job and relatively few entities will actually become HISPs, because it's too expensive and too complicated. That doesn't seem to be scalable for widespread deployment of LOA 3 for doctors and their staff.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

So I think what I also heard you suggesting was the bifurcation of the registration authority functionality versus the certificate authority functionality, right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well, it's almost…I hate to use the registration authority lingo because that brings with it all those policy questions. It's more this organization driven, the organization gets vetted, the organization's representative gets vetted and then that person internally in the organization, follows some rules and obtains credentials for everyone in that organization. That's how direct is working today, once you get…after you get past the organization level. And we chose to go that way because it's less expensive and less complicated in requiring every single person in the hospital to go get…to go through some RA.

So you only…the RA really only applies to the top level part of the organization and its representative. Everyone else is provisioned just like an account on an EHR.

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

In the direct protocol right now though, that protocol only extends to organizational level, it does not specify what the requirements are for the organization to do to ID proof its employees.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

They are working on what would be equivalent to the presenter's definition of do the right thing…

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Yeah, but when you're talking about they are, are you talking about direct trust organizations?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, direct trust and the others that are trying to become HISPs, such as Surescripts and the like. So, the do the right thing language is being worked on. I think it's probably pretty closely compliant to remote proofing as defined by NIST. But it's not going to pass muster with Tony, because it's not a FICAM process yet. So. it seems like we're very close in what's working in the real world and what would be acceptable to FICAM, if we connected the dots. Maybe I'm being optimistic, but it's…

Deven McGraw – Center for Democracy & Technology – Director

Well right, I mean, so some of that is, are the dots connectable. But there's a desire to connect those dots, I wouldn't disagree. I want to make sure we get a few more comments in because we're actually now eating up our time. So, Wes, John and Walter.

Wes Rishel – Gartner, Incorporated

So, it's been very clarifying for me. I think the first lesson that I learned is that nobody trusts anybody absolutely. All right, there's an old joke about friendship, a friend is someone you ask to help you move, a real friend is someone you ask to help you move a body. And, to a certain extent, we're really focusing on purely on who we trust to say that this person is the person on the internet. We're almost immediately getting that confused with who do you trust to do something with, such as make your data available to be pulled from your database about your patients or something like that. And immediately there, we get to problems of revoking the trust. It's arguably not wonderful that we trust that John Edwin Rishel is a person who was born in 1923, in some little town in Illinois, I forget. But the fact that he has been dead for some years is more important if we're trying to send him a check or we're trying to get his assent in order to transfer a land deed or something like that. I don't know how far we get just on pure identity, but I do share sort of a trust, pardon the expression, faith in the basics that says if we were able to do that, it would somehow help us with what do we trust what.

We seem to be really looking at an idea that we used to say we believe, which is commutative trust, I trust this organization to properly manage their employees so that they're not going to breach information they got from me. I trust my HIE, who trusts organizations, but then the question seems to come up in Washington and everywhere else, once you get beyond a certain level, commutativity tends to fall down and if we're looking for an alternative for it, we have to do a lot more than just identify the person. We have to identify the organization; we have to go through a process that we're describing now. I am frankly intimidated by that prospect and tend to be more persuaded by David than I ever have before, that the only two ways information will ever get transferred is by being pushed or being sent through a PHR controller or medical data bank, or something controlled by the patient. This notion that we're going to figure…work out all of these issues is troublesome. Finally, we had three-way boggle about the cost of the process of verifying identity. Innovation in business models in order to cover the cost and standards so that we can operationally share the identity, it's like I used to tell my boss, you can have this software quickly, good or fast, pick two, but if we are going to take advantage of innovative models, that implies less stability to have standards.

I mean maybe there's a magical…David likes to use the metaphor of a cleavage plane in surgery. Cut someone, if you cut this way you don't sever a lot of nerves and blood vessels and things like that, if you cut the other way, it's a mess. Okay, well maybe there's a magic cleavage plane around identity that we can somehow share the results and identity without sharing the whole business process by which we get the identity, but if we don't. if we're going to rely on sort of the staid processes that are sufficiently long to produce standards, we've got to find some other way to cover the cost.

Deven McGraw – Center for Democracy & Technology – Director

Thanks Wes. John?

John Houston – University of Pittsburgh Medical Center

I echo the fact that I think this was a really great dialogue today and great hearing. My mind sort of runs wild as to all the different opportunities and all the different challenges. And I think the thing that I guess would be helpful, at least to me, is really to try…somebody to frame out all the different use cases. Because there are so many different use cases and to Wes' last point, what ends up happening is that each use case, there's a lot of overlap, but they have their own nuances. And to Wes' point, some require more than others in terms of what needs to be provided. Some may require more authentication on the front end or identity proofing on the front end, others…it's just that I think it would be of value to make sure we fully understand what we envision here and in all the different contexts. Because really, I think any given one of us probably has some sense of what…how this is going to play out in terms of an operational environment and where they see the most use and the most value coming from. But each one of those use cases is going to sort of have its own set of criteria and identity proofing requirements and the like. So, I know that sounds like a big exercise, but just trying to lay out all the use cases and then understanding the value of each, so that we can…I don't know if we need to prioritize or maybe we'll still come to the conclusion that we just need to do all of this. But I think it would be helpful to help frame the arguments and the requirements.

Deven McGraw – Center for Democracy & Technology – Director

Thank you. Walter?

Walter Suarez, MD, MPH – Kaiser Permanente

Yeah, just like everybody else, I echo. The very valuable information we received today was just incredible. A couple themes and messages I got out of this, I think, as I said earlier, it gives now the feeling that it's not any more whether, but when and more importantly, how soon. It's not even when in the next five years, but how soon in the next 18-24 months, or something like that. It's really moving very quickly into elevating the level of assurance across the system. The other big theme that I heard was, maybe it's appropriately so because of the title, but this is all about individual level certification and credentialing, more so than the organization level. We spent a lot of time around in the past several months and couple years talking about the organizational level of certification and today was all about really individual level credentialing.

The other thing is, this is not just about healthcare, this is about how this can be applied across multiple industries. So if I'm a physician, I can just basically use my level 3 or class 3 level of assurance to prescribe a controlled substance, just as well as going to some secure system to enter some data, and buy a book from whatever system, if that's needed at that point. But it is important to consider that to mention that this is not just necessarily something about healthcare. The other one, I think, and this is probably a very important one from a policy perspective, is what is the role of government really now. So, what is it that would be the appropriate things that can be done to move that tipping point where we are, and that Tony I think mentioned, we've reached the critical mass perhaps, but how can we move the tipping point? And so, my thinking there is that that is really the critical element it's consider what is the role of government and how can government stimulate that, push the envelope, without forcing and creating a unique path into the system that could stifle actually innovation and things like that.

And the very last point is really the cost, I think Wes mentioned. Even five years ago, the cost of any of this was in the two or even three digit level, now we're in the single digit and going down to cents. And so I think it's a very valuable testimony that we heard today how costs have really gone down significantly to help us implement this. Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Thank you. I apologize to Dave and also the folks on the phone but we're now at 2:55 and we at least have to leave some time for public comment if we hope to end on time. So MacKenzie, you want to work you're magic?

MacKenzie Robertson – Office of the National Coordinator

Sure, thanks. Operator, can you open the lines for public comment. And while we're waiting, if there's anyone in the room that wants to come to the table and do public comment.

Alan Merritt – Altarum Institute

If you would like to make a public comment, and you're listening via your computer speakers, please dial 1-877-70….

Public Comment

Deven McGraw – Center for Democracy & Technology – Director

Oh, I'm sorry, I interrupted the telephone…hold on.

Alan Merritt – Altarum Institute

If you'd like to make a public comment, and you're listening via your computer speakers, please dial 1-877-705-2976 and press *1. Or if you're listening via your telephone, you may press *1 at this time to be entered into the queue.

Deven McGraw – Center for Democracy & Technology – Director

So, I'm going to call on Neville first, only because he wasn't one of the presenters Steve, so thanks.

Neville Pattinson – Smart Card Alliance

Thank you very much for entertaining our public comments. My name is Neville Pattinson, I work for a company called Gemalto, who is digital security. We provide a lot of level 3 and level 4 credentials to

hundreds of countries, governments and enterprises including the PIV and CAC cards and the passport and so forth. Listening to it today very carefully, and clearly you got a lot of good information and a lot of learning going on here. I think there are a lot of terms that need to be understood and defined and your understanding. I liked the discussion from John about the use cases, that's critical here because I think in the course of the discussion we need to define what user needs what access and why, because there are different use cases for different accessing of information. If it needs to be just a key to the door authentication is a key to the door that says, please let me in. The guard at the other side of the door is still going to say, well do I trust you, and if I do trust you, I'm only going to let you into this room or I'm going to give you full run of the building or whatever it is. So, understand that authentication is about requesting access, it doesn't mean you have a right to access and it doesn't mean you have the right to access everything.

Then you need to understand if you need to have confidentiality and privacy protection in this dialogue or this request. Authentication is just the ability to open the door and walk in and potentially get to a certain piece of information. But if that information is then provided to view in clear text or in some form that's imperceptible by…organization, then you've violated confidentiality and privacy. So authentication does not give you the privacy detection potentially. It may just give you the accessibility. You then have to think about the integrity of that information. Is that information now trusted because I've gotten this from this individual, this electronic healthcare record, has anybody tampered with it since it was sent out and I've now received it. How do I know it's still correct? The integrity of that information is critical and there are electronic and cryptographic technologies that can ensure that we've got privacy and confidentiality and you've also got integrity in the form that you know the information has not been tampered with and has been delivered by a trusted party.

So, these are all things we deal with every day in terms of understanding what is required in those use cases, do I just need to get in, or am I going to get in access something, if I'm going to access something, do I get that in a form which is now going to be safe and secure and trustable. A lot of what you discussed today has a risk-based approach. The relying parties are the ones who are going to have to have the policies to decide whether they're going to accept this access, this request or the transmission of information. They had to make sure that they are certain that whoever they're dealing with is something that they can trust, so there is going to be a need to have a community of trust between all the parties involved, be them the patient themselves to the providers, to the relying party. There has to be a framework of trust otherwise it will fall apart. NSTIC is indeed setting that direction, it doesn't have the

Specifications today, it has a fabulous strategy and a fabulous vision and in time it will come. And I think Jeremy said four years, I think I heard him say, is the current timeline. So, two to four years, whatever it may be, NSTIC will have a lot of involvement from industry, not for profit, government and the like, to help define and put that together.

To kind of close off very quickly, and in terms of, I mean I have a few minutes, I would just say that I've never heard of level 3 done in a healthcare environment before, anywhere in the implementations we've done around the world. Every single healthcare-based project, be it for payment, insurance, be it for actual records, have all gone through the same anguishing discussions that you've gone through and they've ended up with level 4. They use hardware technology to do this. And that's because it gives the highest level of assurance, there are lots of standards in place and on that basis, they've all selected that particular area, because it is the most trusted and the most available in terms of all the assurance levels that exist.

Just to give you an idea of the CAC four million…base , PIV three million…base, PIV-I, which is the enterprise…there's about a half a million of those in place and FRAC cards, First Responder Cards, which healthcare professionals have today in some organizations, the cards that they are using, there's now about a half a million of those scattered around the country. So already a lot of drive and lot of existence of level 4 technology. I'm not saying it should not have level 3, but whenever you think of level 3, please say level 3 or more, because you're looking at the option of what's already been established all around, many different organizations. So if you choose level 3 at least allow 4 stronger, or level 4 or above in what you consider. And on that, I shall close my comments.

Deven McGraw – Center for Democracy & Technology – Director

So we have…Steve, since you did have a chance to…I want to see if there are folks on the phone.

MacKenzie Robertson – Office of the National Coordinator

There are no public comments right now.

Deven McGraw – Center for Democracy & Technology – Director

All right, you're on.

Steve Kirsch – OneID – Founder and Chief Technology Officer

Okay. So, identity proofing's a hard problem. I think it would be great if the government were to set a standard and this committee could make a decision or some committee, or some government agency could make a decision in terms of what's acceptable and what's not acceptable. And it doesn't have to be a perfect decision, it never will be, but at least you can draw the line in the sand and start with something and say, hey we'll start with this and modify it over time and having government do that, I think, is the best way to do it, because we trust the government. Government passports, I think, are very well trusted, not only within the US, but internationally as well and yet the government doesn't set standards for issuing passports. You can only get passports if you go to a post office and show specific documents. And so it would great if what we did is we added some biometrics. We have your picture, but adding fingerprints and iris to that and then having that become a digital certificate that anyone could access would go a huge way, so that we don't have to have this duplication of identity proofing all the time. All you have to do is show up in person, produce one of the biometrics that match the government's signed certificate and poof, you're in.

They're doing this and other countries. In India, for example, there's an Aadhar project that takes the whole country of India, and every person is standing in line to get their biometrics put in, because in order to do that, if you get your biometrics in, you can get government benefits. And so everybody wants to do this and so India is doing this now. So, India is way ahead of us in terms of identity proofing and creating that...because once you have these…an identity that you have tied biometrics to an identifier like a number, then it's really, really easy to do. So, I would encourage you to take a look at what India is doing and have it be an optional thing where people when they apply for a passport, can add these things and get a digital certificate of their passport, and that would go a long way to solving the identity proofing problem. You solve it once, for all people rather than do a specific point solution. Because I wonder, even today, would you accept passports as identity…a valid identity? Would you accept a driver's license? I mean, pick something, because otherwise you're going to go back and forth saying that's not a good…there's no right answer. Just pick something.

Deven McGraw – Center for Democracy & Technology – Director

If only we had that kind of power. But we do get to do some recommendations, so we appreciate the input on that. So, thank you all very much, we just went a little bit over, that's not too bad. And for Tiger Team members and for members of the public who are interested, our call is next Monday. It's an afternoon call, 2:00 Eastern time, I think we have 90 minutes for this one and the subsequent call that's two hours long to try to wrap this up. I will certainly take any additional thoughts that you have by e-mail to help me shape the agenda and that doubly goes out to you Dave, since I didn't give you a chance to chime in. But I just want to say thank you to everybody and thank you in particular to my partner in crime, Dixie for helping out with this and thank you to the staff, who just put in an enormous amount of time to pull this altogether. Everybody safe travels back and talk to you soon.

Public Comment Received During the Meeting

1. Direct can support both Org level and Indiv level certs
2. When using Org cert, HISP is required to manage the individual authentication of initiators of the transaction
3. If Kaiser was a contracted RA to DigiCert they could certainly do the ID vetting and be issued an FBCA cross-certified credential if appropriate controls are in place